Information Security Policies

+ Glossary and Reference Manual

Securing Information in the Digital Age

Thank you for evaluating the RUSecure™ Information Security Policies

If you wish to re-publish these information security policies, you may purchase the company-wide registered version from our online order page at
http://www.eon-commerce.com/rusecure

The RUSecure™ Information Security Suite

Information Security policies are the foundation - the bottom line - of information security within a modern organisation. As such, it is well worth considering the following few questions :

- Are they comprehensive enough? Are they up to date?
- Do you deliver them effectively (e.g.: via the desktop)?
- How do users comply with the Policies in day-to-day situations?

The **RUSecure™ Information Security Suite** is intended to help you ensure that you can answer these questions positively and confidently. It provides expert guidance to everyone in the organisation and offers solutions to ensure that you not only have complete policies, but that they are delivered effectively and professionally to all concerned via a unique set of tools.

Information Security Policies	A comprehensive, up-to-date set of Information Security Policies that can be tailored to meet the individual needs of your organisation. Shipped in PDF and Microsoft Word formats, they can be used 'as is' or may be copied and modified as you require.
Security Online Support Desktop delivery of your policies	The most direct method of delivering information security policies is via the computer desktop. This carries many benefits, including: • Instant availability for every member staff who handles information • Awareness and guidance built around each Policy • Using the power of a PC to make the experience richer and more productive **RUSecure™ SOS brings your security policies to life!**

Information Security Officer's Manual For the Information Security Professional	The Information Security Officer has an extremely demanding role, and may not always have a dedicated team to support the implementation of Information Security within the organisation. The job is made easier with the right supporting tools. The **Information Security Officer's Manual** is a must-have desktop accessory in every security officer's tool kit. Comprehensive support.... containing a wealth of useful information and guidance. The de facto guide to security management.

Evaluations of each of the products can be obtained from:
http://www.computer-security-policies.com/download.htm

Further Information:
sales@computer-security-policies.com

RUSecure™ - Information Security Policies

Important Note for Evaluators
This evaluation version, whilst delivering the Information Security Policies in their complete form, will not permit the printing or copying of the policies. However, the instructions for use are taken directly from the registered version to permit review of the implementation process.
The registered version of the *RUSecure*™ - Information Security Policies has no printing or copying restrictions and licenses unrestricted use within your organisation.

***RUSecure*™** is a suite of integrated products which, together, offer your organisation the tools necessary to integrate Information Security best practice into your day-to-day business operations. Whether you are a large corporation or a small company with a handful of employees, ***RUSecure*™** offers the assistance needed to secure your information – in this digital age.

Information Security Policies are the cornerstone of Information Security effectiveness. Without a policy upon which to base standards and procedures, decisions are likely to be inconsistent and security holes will be present - ready to be exploited by both internal and external persons alike.

Traditionally, Information Security Policies have only been found in larger organisations which either have dedicated IT and Security staff, or where the organisation has invested a substantial sum in consultants who, over a period of time, will have created and delivered a range of policies for management to implement.

***RUSecure*™** Information Security Policies have been drawn from the extensive experience of senior Information Security consultants who have delivered business systems projects across the world, and where Information Security has played a major role. Based upon the foundation of **ISO 17799** and **BS 7799**, ***RUSecure*™** Information Security Policies provide an extensive range of policies which may be modified and adopted by your organisation and upon which a comprehensive Information Security culture may be built.

Following adoption of the Information Security Polices – either revised or ‘as is’, the primary objective is to have them understood and followed by the organisation’s staff. Some organisations already have an Intranet for the mass distribution of information. However, whilst this approach may be effective in some organisations, in others it is little more than an electronic message board, the contents of which few will actively study.

It was for this reason that Glendalesystems.com Ltd developed the ***RUSecure™*** - **Security Online Support** system which has been designed to deliver each of the Information Security Policies directly to the desktop in a meaningful and practical manner; more importantly, each Policy is delivered *in context*. If you would like to know more about the Security Online Support system simply contact us.

N.B. The numbering system used for these Information Security Policies matches the numbering within the ***RUSecure™*** - **Security Online Support** system to facilitate future upgrade and migration.

Contents

USING YOUR INFORMATION SECURITY POLICIES

The purchase of ***RUSecure™ - Information Security Policies*** is a major step towards a comprehensive, consistent and meaningful security conscious environment within your organisation. Recent studies have shown that **85% of organisations have no formal set of Information Security Policies** and, as a result there is little or no foundation upon which to build the appropriate safeguards to protect the life blood of the organisation – its information.

Expected Reader / User

One of the key appointments in **any** organisation – irrespective of size or function, is to appoint an **Information Security Officer**. Except in the larger organisations, this person is unlikely to be a full time specialist; on the contrary, they are likely to be performing a role that is business related. The point is, **someone** must be appointed to take the overall responsibility for ensuring that the appropriate Information Security safeguards are in place, that Polices are agreed and rolled-out, and that all users of information within your organisation understand their responsibilities and duties. For the purposes of the ***RUSecure™ - Information Security Policies*** and their optimum use within your organisation, we assume that you have, or will make, such an appointment within your organisation. For further information and a comprehensive guide to the role and responsibilities of the **Information Security Officer**, you may wish to consider the Information Security Officer's Manual – a key ***RUSecure™*** Information Security support tool.

Other Expectations

Whilst the following Information Security Policies lay a solid foundation for the development and implementation of secure practices within your organisation, the Policies themselves are not instructional or overly descriptive. They represent the rules which must be adhered to by the organisation. Such **compliance** will require an understanding by staff of not only the individual policies but also of the circumstances in which such compliance is expected in their day-today activities. Knowing the Policies is only one half of the equation - staff need to know ***how*** they should comply, from a procedural perspective.

For this reason, version 2.0 of the Information Security Policies includes these additional 3 **key features** :-

1) **Explanatory Notes** providing background to the Policy
2) Some of the **Key Information Security Issues** which should be considered when implementing the Policy in question
3) The **Related ISO 17799 / BS 7799** reference(s). The British Standard for Information Security was, in October 2000 approved as an ISO standard. This document is a key standard against which Information Security standards can be measured. The references within ***RUSecure™***

Information Security Policies ensure that easy cross referencing is possible.

The Steps to Implementation

In the following Chapters, you will find headings which relate to logical groupings e.g. the first chapter is concerned with the security of hardware, peripherals and other equipment. Within each chapter there are appropriate sub chapters again group related items. Following these are the individual Information Security Policies. The Policies themselves have been drawn from the extensive experience of IT and Security professionals and are based upon the renowned International Standards of BS 7799 and ISO 17799. Moreover, whilst the Policies do not claim to cover every conceivable area of information systems, their scope is more than adequate to lay the foundation for an organisation operating in accordance with accepted international best practice.

There are **six steps** involved in getting the best from ***RUSecure™* - Information Security Policies**. Follow these steps and the risks from Information Security related incidents can be reduced – measurably.

Step 1 – Browse the Policies

The first step is to print out the Information Security Policies from this document. Start at page 13 and print up to and including the last policy on page 396.

Work through each of the main Chapter headings and confirm that it is relevant to your organisation. It is not necessary to consider Information Security Policies which relate to areas and functions beyond the scope of your normal (or anticipated) commercial operations. For example, if you have never (and plan never) to write (or have written) your own business software, the Information Security Policies relating to Developing and Maintaining In-House Software may be omitted. However, such decisions will usually need to be confirmed at Board / Director level.

Step 2 – Study the Policies

The majority of the Chapters and Sub Chapters will be relevant to **any** organisation. Think long and hard about excluding areas. It may be that some aspects of your organisation's operations are less familiar to you. In such cases, you should discuss the scope of the Policies with colleagues who represent each of the key functional / business areas.

Study each Policy within the context of the heading. Whilst the wording is as 'jargon free' as possible, it is still likely that some terms may not be totally familiar to you. For this reason, we have embedded links to a comprehensive **Glossary and Reference** manual (which follows the Policies) which will hopefully answer any immediate queries.

Step 3 – Review and Amend the Policies

Whilst the Policies have been developed to be applicable to the majority of organisations, there are key aspects that may need your attention. For example, some Policies make specific reference to Legislation e.g. adherence to the Data Protection Act. If your country has its own alternative legislation, then the Policy needs to reflect this. Likewise, in the area of Human Resources, legislation that is specific to your country **or industry** may result in the need to enhance the wording of the Policy concerned.

In the majority of cases however, we anticipate your being able to agree to the wording as presented, which should make this part of the process quick and easy. We suggest that you replace the generic term 'organisation' (used throughout ***RUSecure™***) with your company or organisation name; conveying a sense of ownership.

Step 4 – Confirm / Ratify the Policies

For Policies to be effective, with compliance mandatory, they must be supported and ratified by your Board of Directors or similar governing body. This agreement is likely to require an outline of precisely ***how*** compliance will be achieved and the management procedures to be put in place to monitor and manage the process. Your organisation may already have such procedures in place, but if not, you may require some additional support. (The ***RUSecure™*** - Information Security Officer's Manual is one such source).

Step 5 – Publish the Policies

The Policies will now have been discussed, agreed and passed by your Board of Directors or similar, and may now be published to all staff. The head of Human Resources / Personnel must be one of the first recipients as employment contracts may need to be amended to reflect the mandatory need for compliance with the organisation's Information Security Policies.

Traditionally, Information Security Policies have been delivered in paper form either to each member of staff or to the Head of Department (or similar) with staff being required to read and then sign to demonstrate their awareness.

Step 6 – Implement / Comply with The Policies

Implementation, compliance and follow up are now required. The Information Security Policies have established the ground rules across a wide range of Information Security areas. But translating these into a meaningful and practical response to the various day-to-day situations by your personnel, can be a challenge. The most important aspect of Information Security Policy compliance is knowing what actions are required to constitute 'compliance'. Your organisation must either develop its own range of procedures or consider using a tool specially crafted for the job.

In addition, the requirements of the Policies will result in the need to initiate one or more Information Security **Projects** to identify and implement a range of appropriate technical safeguards such as firewalls, anti virus software, intrusion detection systems etc.

If you have any comments or queries relating to any of these Information Security Policies please feel free to contact us via e-mail and we shall be pleased to help.

CHAPTER 01
SECURING HARDWARE, PERIPHERALS AND OTHER EQUIPMENT

Sub-Chapter 01
Purchasing and Installing Hardware

Policy 010101
Specifying Information Security Requirements for New Hardware

SUGGESTED POLICY STATEMENT

"All purchases of new systems hardware or new components for existing systems must be made in accordance with Information Security and other organisation Policies, as well as technical standards. Such requests to purchase must be based upon a User Requirements Specification document and take account of longer term organisational business needs."

EXPLANATORY NOTES

The purchase of new computers and peripherals requires careful consideration of your business needs because it is usually expensive to make subsequent changes.

Information Security issues to be considered when implementing your policy include the following:

- The system must have adequate capacity or else it may not be able to process your data.
- Data must be adequately protected; otherwise there is a risk of loss or accidental / malicious damage.
- Where hardware maintenance is poor or unreliable, you greatly increase the risk to the organisation, because, in the event of failure, processing could simply STOP.
- The system must be sufficiently 'resilient' to avoid unplanned *down-time*, which can have an immediate negative impact on your organisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.4 Authorisation process for information processing facilities

Policy 010102
Specifying Detailed Functional Needs for New Hardware

SUGGESTED POLICY STATEMENT

"Except for minor purchases, hardware must be purchased through a structured evaluation process which must include the development of a detailed Request For Proposal (RFP) document. Information Security features and requirements must be identified within the RFP."

EXPLANATORY NOTES

It is necessary to specify, in detail, the specific functional performance and capacity requirements as part of the hardware purchasing process. The document specifying these detailed requirements is usually called a Request for Proposal or 'RFP'. See *Request for Proposal* for a more detailed description of how to create such a document

Information Security issues to be considered when implementing your policy include the following:

- Where hardware is purchased without adequate analysis your organisation may:-

    1) Purchase inappropriate hardware for the required task.

    2) Purchase a system that does not comply with your *Technical Architecture* or *IT Strategy*.

    3) Fail to achieve the best value when (e.g.) price, performance, reliability, capacity and support issues are considered

    4) Supply confidential information to a vendor which can lead to commercial damage thorough unauthorised disclosure.
- A number of comparable bids are necessary to make an informed comparison and purchase appropriately; without these you risk a sub-optimum quote.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.4 Authorisation process for information processing facilities

Policy 010103
Installing New Hardware

SUGGESTED POLICY STATEMENT

"All new hardware installations are to be planned formally and notified to all interested parties ahead of the proposed installation date. Information Security requirements for new installations are to be circulated for comment to all interested parties, well in advance of installation."

EXPLANATORY NOTES

Installation of new equipment must be properly considered and planned to avoid unnecessary disruption and to ensure that the Information Security issues are adequately covered.

Information Security issues to be considered when implementing your policy include the following:

- The equipment must be located in a suitable environment otherwise it may fail.
- Any disclosure of your network diagrams, security features, locations, configurations etc. exposes potential vulnerabilities which could be exploited.
- Leaving software tools, utilities and developer's kits on your new system endangers the confidentiality and integrity of your data.
- Without an installation plan for the new equipment, disruption to operational systems is more likely.
- Where the installation plan does not include safeguards against the (inevitable) increased security threat resulting from (relatively) 'open access' to the systems area, accidental or malicious damage can result.
- Breaches of Health and Safety regulations endanger the well-being of your staff and your organisation's commercial activities.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.4 Authorisation process for information processing facilities

Policy 010104
Testing Systems and Equipment

SUGGESTED POLICY STATEMENT

"All equipment must be fully and comprehensively tested and formally accepted by users before being transferred to the live environment."

EXPLANATORY NOTES

Hardware should be tested when new to verify it is working correctly, and then further tests applied periodically to ensure continued effective functioning.

Information Security issues to be considered when implementing your policy include the following:

- Where new equipment is not tested for critical functions before being used, it can lead to failure and hence damage to both data and other linked systems.
- Inadequate testing can threaten the integrity and availability of your data.
- Where testing is performed in a manner that does not simulate live conditions, the results of such testing cannot be relied upon.
- Poor security procedures during equipment testing can compromise the confidentiality of your data.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.4 Authorisation process for information processing facilities

Sub-Chapter 02
Cabling, UPS, Printers and Modems

Policy 010201
Supplying Continuous Power to Critical Equipment

SUGGESTED POLICY STATEMENT

"An Uninterruptible Power Supply is to be installed to ensure the continuity of services during power outages."

EXPLANATORY NOTES

An *Uninterruptible Power Supply* is a critical hardware component which enables continuity of function in the event of a power failure.

Information Security issues to be considered when implementing your policy include the following:

- If the mains power fails for any reason, your system will crash and data files may be corrupted.
- A malfunctioning UPS may cause your systems to crash in an uncontrolled manner following a mains electrical failure. Such crashes can often corrupt data files.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.2 Power Supplies

Policy 010202
Managing and Maintaining Backup Power Generators

SUGGESTED POLICY STATEMENT

"Secondary and backup power generators are to be employed where necessary to ensure the continuity of services during power outages."

EXPLANATORY NOTES

The issues that arise when standby generators are used as a safeguard against mains electricity failure. Such generators are usually employed with *Uninterruptible Power Supplies*.

Information Security issues to be considered when implementing your policy include the following:

- If the mains power supply fails, and the generator malfunctions, your system will crash, not only probably losing current data, but also the data file(s) open at the time. Such an event can turn a potentially small incident into a disaster.
- Without a generator, any UPS will drain its battery charge within a relatively short period, thus preventing systems' usage during a prolonged power failure.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.2 Power Supplies

Policy 010203
Using Fax Machines / Fax Modems

SUGGESTED POLICY STATEMENT

"Sensitive or confidential information may only be faxed where more secure methods of transmission are not feasible. Both the owner of the information and the intended recipient must authorise the transmissions beforehand."

EXPLANATORY NOTES

This policy considers the threats associated with the use of fax machines. The risks stem primarily from the relative insecurity of the medium.

Information Security issues to be considered when implementing your policy include the following:

- Confidential data can be disclosed to unauthorised persons.
- Fraudulent incoming messages may result in action being taken that is detrimental to your organisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.5 Security of electronic office systems
8.7.7 Other forms of information exchange

Policy 010204
Using Modems / ISDN / DSL connections

SUGGESTED POLICY STATEMENT

"Sensitive or confidential information may only be sent via public telephone lines where more secure methods of transmission are not feasible. Both the owner of the information and the recipient must authorise the transmission beforehand."

EXPLANATORY NOTES

This policy relates to the potential dangers arising when using Modems, ISDN links and DSL connections to access the public telephone network to link geographically diverse parts of your computer systems.

Information Security issues to be considered when implementing your policy include the following:

- These services provide an instant extension of your network, but use insecure public lines and therefore increase the risk of attack.
- Data transmitted over such connections may be exposed during transmission.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.5 Security of electronic office systems

Policy 010205
Using Centralised, Networked or Stand-Alone Printers

SUGGESTED POLICY STATEMENT

"Information classified as Highly Confidential or Top Secret, may never be sent to a network printer without there being an authorised person to safeguard its confidentiality during and after printing."

EXPLANATORY NOTES

Printers output information on a continual basis in many offices, and the content of that information can vary from inconsequential intra-office notices, to highly confidential information with a restricted circulation.

Information Security issues to be considered when implementing your policy include the following:

- Confidential information may be revealed to unauthorised persons.
- Pre-printed computer stationery may be used fraudulently.
- Printer malfunctions can result in unintelligible output; especially where multiple language fonts are being used.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.3.1(f) Clear desk and clear screen policy
8.6 Media handling and security

Policy 010206
Installing and Maintaining Network Cabling

SUGGESTED POLICY STATEMENT

"Network cabling should be installed and maintained by qualified engineers to ensure the integrity of both the cabling and the wall mounted sockets. Any unused network wall sockets should be sealed-off and their status formally noted."

EXPLANATORY NOTES

Network cabling remains a vulnerable target as in many organisations it is exposed and unprotected.

Information Security issues to be considered when implementing your policy include the following:

- Malicious damage to networks can cause disruption to processing and communications.
- Illegal tapping of networks can compromise your data and security measures, such as user names and passwords.
- Accidental damage to network cables can threaten data processing.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.3 Cabling security

Sub-Chapter 03
Consumables

Policy 010301 **Controlling IT Consumables**

Policy 010302 **Using Removable Storage Media including Diskettes and CDs**

Policy 010301
Controlling IT Consumables

SUGGESTED POLICY STATEMENT

"IT Consumables must be purchased in accordance with the organisation's approved purchasing procedures with usage monitored to discourage theft and improper use."

EXPLANATORY NOTES

Examples of consumables are printer forms, stationery, printer paper, toner and ribbons.

Information Security issues to be considered when implementing your policy include the following:

- Pilfering of your consumables results in increased organisational expense.
- Consumables may be stolen with the intent to defraud your organisation or customers.
- Confidential data may be revealed to unauthorised persons from discarded consumables, e.g. discarded draft printer output

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.1 Management of removable computer media

Policy 010302
Using Removable Storage Media including Diskettes and CDs

SUGGESTED POLICY STATEMENT

"Only personnel who are authorised to install or modify software shall use removable media to transfer data to / from the organisation's network. Any other persons shall require specific authorisation."

EXPLANATORY NOTES

When using removable storage media, there are additional Information Security risks associated with the portability of the media.

Information Security issues to be considered when implementing your policy include the following:

- Loss or 'disappearance' of disks, tapes, etc. can compromise the confidentiality of the organisation's data.
- Damage to media compromises the integrity of your corporate records.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6 Media handling and security

Sub-Chapter 04
Working Off Premises or Using Outsourced Processing

Policy 010401
Contracting or Using Outsourced Processing

SUGGESTED POLICY STATEMENT

"Persons responsible for commissioning outsourced computer processing must ensure that the services used are from reputable companies that operate in accordance with quality standards which should include a suitable Service Level Agreement which meets the organisation's requirements."

EXPLANATORY NOTES

The following issues should be considered if your organisation decides to outsource some or all of its computer processing.

Information Security issues to be considered when implementing your policy include the following:

- Inadequate performance can threaten your organisation's information processing and business operations.
- Poor reliability can threaten the performance of your business.
- Lack of direct control when outsourcing can compromise data confidentiality.
- Inadequate controls to assure legal compliance, e.g. Data Protection regulations.
- Inadequate Disaster Recovery plans can terminate your organisation's commercial activities in the event of an unforeseen problem.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.3.1 Security requirements in outsourcing contracts
10.5.5 Outsourced software development

Policy 010402
Issuing Laptop / Portable Computers to Personnel

SUGGESTED POLICY STATEMENT

"Line management must authorise the issue of portable computers. Usage is restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices."

EXPLANATORY NOTES

Laptops, Portables, Palmtops - even electronic 'organisers' which connect to and store your organisation's data - are included within this policy. Collectively, they are referred to as portable computers.

Information Security issues to be considered when implementing your policy include the following:

- Confidential data disclosed to unauthorised persons can damage the organisation.
- The use of unlicensed software can subject your organisation to legal action.
- *Viruses*, *Worms*, *Trojans* and other *Malicious code* can corrupt both data and the system files.
- Theft of the portable computer exposes the organisation to the threat of disclosure of sensitive corporate data to competitors.
- Inadequate backup and recovery routines can lead to the loss of data.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.8.1 Mobile computing

Policy 010403
Using Laptop / Portable Computers

SUGGESTED POLICY STATEMENT

"Persons who are issued with portable computers and who intend to travel for business purposes must be made aware of the information security issues relating to portable computing facilities and implement the appropriate safeguards to minimise the risks."

EXPLANATORY NOTES

Laptops and Portables have unique security issues, primarily because of their size and mobility.

Information Security issues to be considered when implementing your policy include the following:

- Confidential data disclosed to unauthorised persons can damage the organisation.
- A virus threatens not only the data but also the system files on the laptop.
- A laptop connected to any network is open to hacking and is unlikely to have any effective security features enabled. Files and data could be stolen, damaged, or corrupted.
- A laptop left 'on' may be easy prey to opportunist access, despite your use of (say) a user password etc.
- Theft of a laptop computer usually results in additional cost to the organisation and potential loss of confidential data.
- Where a laptop is used by persons with differing *access control* privilege, residual data and / or other information could compromise the confidentiality of your information.
- When vital updates to the data files are lost or corrupted due to technical or user problems during transfer, the integrity of the entire database of records may be in question.
- Where a laptop is used by several persons, old / 'stale' data may still be present, risking unintentional actions / reactions to inaccurate data.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.5 Security of equipment off-premises
9.8.1 Mobile computing

Policy 010404
Working from Home or Other Off-Site Location (Tele-working)

SUGGESTED POLICY STATEMENT

"Off-site computer usage, whether at home or at other locations, may only be used with the authorisation of line management. Usage is restricted to business purposes, and users must be aware of and accept the terms and conditions of use, which must include the adoption of adequate and appropriate information security measures."

EXPLANATORY NOTES

Tele-working is where staff work from home, or another nominated location, away from the normal office environment. See '*Day to Day Use of Laptop / Portable Computers*', which is also likely to be relevant to staff who are tele-working.

Information Security issues to be considered when implementing your policy include the following:

- Viruses are likely to destroy the integrity of your data and possibly of your entire system.
- The use of any unlicensed software, for the purposes of processing the organisation's information, could result in legal action.
- Confidential data may be exposed to unauthorised persons.
- Incompatible software versions can cause problems and even data corruption. See also *Upgrading Software*.
- Data and information can be destroyed, deleted, or otherwise corrupted, on a home PC.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.5 Security of equipment off-premises
9.8.2 Teleworking

Policy 010405
Moving Hardware from One Location to Another

SUGGESTED POLICY STATEMENT

"Any movement of hardware between the organisation's locations is to be strictly controlled by authorised personnel."

EXPLANATORY NOTES

The physical removal and relocation of hardware from one location to another.

Information Security issues to be considered when implementing your policy include the following:

- Confidential data may be exposed to unauthorised persons, threatening the confidentiality of sensitive information.
- Equipment can be damaged in transit.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2 Equipment security

Policy 010406
Using Mobile Phones

SUGGESTED POLICY STATEMENT

"Personnel issued with mobile phones by the organisation are responsible for using them in a manner consistent with the confidentiality level of the matters being discussed."

EXPLANATORY NOTES

Otherwise known as 'cell phones', 'portable phones' or 'hand phones', mobiles are being used more and more to communicate business information, and it has not gone unnoticed by those wishing to 'tap' or otherwise corrupt such information flow.

Information Security issues to be considered when implementing your policy include the following:

- Theft of a mobile could result in the disclosure of confidential information to the 'new user'.
- Confidential information may be overheard and / or tapped into.
- Relying upon the information in a text message sent to your mobile can result in inappropriate action / decisions.
- Where mobiles are used by various persons, inappropriate personal calls to the mobile can aggravate business usage.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.5 Security of equipment off-premises
8.7.5 Security of electronic office systems

Policy 010407
Using Business Centre Facilities

SUGGESTED POLICY STATEMENT

"Personnel using business centres to work on the organisation's business are responsible for ensuring the security and subsequent removal and deletion of any information entered into the business centre's systems."

EXPLANATORY NOTES

Business centres are computing facilities often provided by hotels for the use of their guests or others. The chief threats posed by such facilities are those of inadequate access controls and the lack of confidentiality.

Information Security issues to be considered when implementing your policy include the following:

- Viruses and malicious code may destroy the integrity of your data and system(s).
- Documents and files can remain on an insecure system over which you have no control.
- Screens may easily be overlooked, and the contents noted.
- Any printed output is left exposed pending retrieval, which can expose the contents of the screen/work area.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.8.1 Mobile computing

Policy 010408
Day to Day Use of Laptop / Portable Computers

SUGGESTED POLICY STATEMENT

"Laptop computers are to be issued to, and used only by, authorised employees and only for the purpose for which they are issued. The information stored on the laptop is to be suitably protected at all times."

EXPLANATORY NOTES

Because of their small size and high value, laptop computers make attractive targets for thieves. A recent survey from the Computer Security Institute showed that laptop theft ranked third on a list of high-tech criminal activities. There are two main areas of concern for those using laptops: (1) avoiding the loss or theft of a laptop and (2) protecting sensitive data in the case of a theft.

Information Security issues to be considered when implementing your policy include the following:

- Confidential data may be exposed to unauthorised users.
- The laptop is lent to family or friends for personal use exposing the programs and data to possible misuse and / or altered configuration and settings.
- A laptop in your custody may be stolen or misused.
- Where laptops on loan have files which have been inappropriately locked using password protection, frustration and resource wastage occurs in trying to access the data.
- Where a lack of policy exists regarding purchase or use of laptops, this may result in indiscriminate use of laptops and data.
- Where laptops are issued, but not signed for, it may result in difficulty in tracing items and ensuring their return when needed.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.8.1 Mobile computing

Sub-Chapter 05
Using Secure Storage

Policy 010501 **Using Lockable Storage Cupboards**

Policy 010502 **Using Lockable Filing Cabinets**

Policy 010503 **Using Fire Protected Storage Cabinets**

Policy 010504 **Using a Safe**

Policy 010501
Using Lockable Storage Cupboards

SUGGESTED POLICY STATEMENT

"Sensitive or valuable material and equipment must be stored securely and according to the classification status of the information being stored."

EXPLANATORY NOTES

A lockable storage cupboard should be considered for storing sensitive or valuable equipment.

Information Security issues to be considered when implementing your policy include the following:

- Information which may be sensitive / of value to the organisation, may be stolen from your premises.
- Sensitive / valuable information, although in a cabinet, may nevertheless be stolen or damaged whilst stored on your premises.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.1.3 Securing offices, rooms and facilities

Policy 010502
Using Lockable Filing Cabinets

SUGGESTED POLICY STATEMENT

"Documents are to be stored in a secure manner in accordance with their classification status."

EXPLANATORY NOTES

A lockable filing cabinet should be considered for secure storage of paper based files and records, or small but movable items.

Information Security issues to be considered when implementing your policy include the following:

- Unsecured sensitive material may be stolen from your premises.
- Sensitive material, despite being placed in lockable filing cabinets, may be stolen or damaged whilst stored on your premises.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.1.3 Securing offices, rooms and facilities

Policy 010503
Using Fire Protected Storage Cabinets

SUGGESTED POLICY STATEMENT

"Documents are to be stored in a secure manner in accordance with their classification status."

EXPLANATORY NOTES

A fire protected storage cabinet is a good way to protect sensitive material against the risk of being destroyed by fire and possible water damage from fire fighting activities.

Information Security issues to be considered when implementing your policy include the following:

- Sensitive data stored in fire-protected cabinets can nevertheless be damaged beyond use.
- Due to their possible additional weight, siting is a key consideration.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.1.3 Securing offices, rooms and facilities
7.3.1(b) Clear desk and clear screen policy

Policy 010504
Using a Safe

SUGGESTED POLICY STATEMENT

"Documents are to be stored in a secure manner in accordance with their classification status."

EXPLANATORY NOTES

The security of sensitive and confidential organisation material is very important and the use of safes for storage is to be encouraged. The security of the safe itself is just as critical.

Information Security issues to be considered when implementing your policy include the following:

- Sensitive data may be lost if the whole safe is stolen.
- The siting of the safe is critical and must not lend itself to lengthy periods of non-surveillance.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.1.3 Securing offices, rooms and facilities
7.3.1(a) Clear desk and clear screen policy

Sub-Chapter 06
Documenting Hardware

Policy 010601 **Managing and Using Hardware Documentation**

Policy 010602 **Maintaining a Hardware Inventory or Register**

Policy 010601
Managing and Using Hardware Documentation

SUGGESTED POLICY STATEMENT

"Hardware documentation must be kept up-to-date and readily available to the staff who are authorised to support or maintain systems."

EXPLANATORY NOTES

'Documentation' refers to both the operator manuals and the technical documentation that should be provided by the supplier / vendor.

Information Security issues to be considered when implementing your policy include the following:

- If equipment is operated incorrectly mistakes and damage may result.
- A failure to follow the recommended schedule of maintenance runs the risk of system malfunction, which could possibly jeopardise your business operation.
- Failure to operate equipment in accordance with the instructions can invalidate the warranty.
- Failure to complete and return the manufacturer's warranty card may invalidate the warranty and hence limit the manufacturer's liability.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.1.1(a) Inventory of assets
8.6.4 Security of system documentation

Policy 010602
Maintaining a Hardware Inventory or Register

SUGGESTED POLICY STATEMENT

"A formal Hardware Inventory of all equipment is to be maintained and kept up to date at all times."

EXPLANATORY NOTES

A register / data base of all computer equipment used within your organisation is to be established and maintained.

Information Security issues to be considered when implementing your policy include the following:

- Theft of equipment is most likely to result in additional cost to the organisation and could compromise data security.
- Inadequate insurance could render your organisation liable to loss in the event of a claimable event.
- Shortcomings in the planning of equipment replacement, can make it difficult to plan ahead for new technology.
- Where documentation is poor, or perhaps non existent, the planning and performance of upgrades to equipment can be both time consuming and also fraught with problems.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.1.1 Inventory of assets

Sub-Chapter 07
Other Hardware Issues

Policy 010701
Disposing of Obsolete Equipment

SUGGESTED POLICY STATEMENT

"Equipment owned by the organisation may only be disposed of by authorised personnel who have ensured that the relevant security risks have been mitigated."

EXPLANATORY NOTES

This policy deals with the issues that should be addressed when disposing of your computer equipment, either for use by others, or for scrap / re-cycle.

Information Security issues to be considered when implementing your policy include the following:

- Legacy data from old systems can still remain accessible and thus compromise the confidentiality of information.
- Inadequate planning for the disposal and upgrade of entire systems can threaten business continuity and result in severe loss.
- Equipment used periodically but infrequently may be disposed of accidentally.
- Breaches of health and safety requirements threaten the well-being of your staff and render you liable to prosecution.
- The disposal of old equipment can prevent the restoration of its associated data files on which you may be relying.
- During the legitimate disposal of unwanted equipment other items can be 'lost' or stolen.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.6 Secure disposal or re-use of equipment

Policy 010702
Recording and Reporting Hardware Faults

SUGGESTED POLICY STATEMENT

"All information system hardware faults are to be reported promptly and recorded in a hardware fault register."

EXPLANATORY NOTES

Hardware faults are to be recorded and reported to the appropriate trained staff or maintenance firms for corrective action.

Information Security issues to be considered when implementing your policy include the following:

- No procedures in place to handle hardware fault reporting will result in ad-hoc and variable response and record keeping.
- Insufficient data may result in incorrect diagnosis of the fault or a possible security breach.
- Lack of any proactive preventative maintenance.
- Failure to identify a 'pattern' of problems and faults can delay remedying the problem.
- Failure to record faults can impede a claim against the manufacturer or vendor. Errors may be compounded due to delays in fault or incident reporting.
- No procedures in place to handle hardware fault reporting, recording, and maintenance.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.4 (c) Equipment maintenance
8.4.3 Fault logging

Policy 010703
Insuring Hardware

SUGGESTED POLICY STATEMENT

"All computing equipment and other associated hardware belonging to the organisation must carry appropriate insurance cover against hardware theft, damage, or loss."

EXPLANATORY NOTES

The need to provide adequate insurance for your hardware.

Information Security issues to be considered when implementing your policy include the following:

- Your business may be compromised, and possibly jeopardised, if systems are not available and adequate insurance cover is not available when needed.
- Financial loss may arise from inadequate insurance cover.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.4 (d) Equipment maintenance
7.2.5 (d) Security of equipment off-premises

Policy 010704
Insuring Laptops / Portables for use Domestically or Abroad

SUGGESTED POLICY STATEMENT

"All portable computing equipment is to be insured to cover travel domestically or abroad."

EXPLANATORY NOTES

There are additional Information Security issues in respect of insuring mobile hardware, including the impact of potential theft and damage to information and data.

Information Security issues to be considered when implementing your policy include the following:

- Shortfalls in the extent of the cover may lead to unexpected losses for your organisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.4 (d) Equipment maintenance
7.2.5 (d) Security of equipment off-premises

Policy 010705
Clear Screen Policy

SUGGESTED POLICY STATEMENT

"All users of workstations, PCs / laptops are to ensure that their screens are clear / blank when not being used."

EXPLANATORY NOTES

With open plan offices becoming common you could accidentally expose confidential material. Information can be read from your screen, especially when your workstation is logged on and you are away from your desk. A *Clear Screen Policy* is an effective safeguard.

Information Security issues to be considered when implementing your policy include the following:

- If your screen is readable when you are absent from your desk or work area, this may result in sensitive information being read and 'leaked' to unauthorised persons.
- When people can see when a sensitive system is being accessed, it facilitates either pre-meditated or opportunistic attempts to read and copy the data when the PC is left unattended; even for a short period.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.1 Secure areas
7.3.1 Clear desk and clear screen policy

Policy 010706
Logon and Logoff from your Computer

SUGGESTED POLICY STATEMENT

"Approved login procedures must be strictly observed and users leaving their screen unattended must firstly lock access to their workstation or log off."

EXPLANATORY NOTES

The access to the vast majority of systems is via a logon process. The security of the system is therefore highly dependant on suitable logon and logoff procedures. See also *Access Control*.

Information Security issues to be considered when implementing your policy include the following:

- Unauthorised access to systems may be gained via a valid user ID and password if these are not kept secure.
- Incorrect logon scripts and access rights may allow access to unauthorised areas.
- Unauthorised access to files may result in the confidentiality of data being compromised.
- Where the 'User Logon Register' or operator / administrator logs show incorrect or unusual entries, it could indicate that data has been accessed and therefore possibly lost or stolen.
- You may be unable to logon to the system and denied service.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.3.1(c) Clear desk and clear screen policy
9.2 User access management

Policy 010707
Dealing with Answering Machines / Voice Mail

SUGGESTED POLICY STATEMENT

"Sensitive or confidential information must not be recorded on Answering Machine / Voice Mail systems."

EXPLANATORY NOTES

Answering machines and Voice Mail are used to record a message because the called party is unavailable to take your call. Leaving confidential information on an answering machine can result in a breach of confidentiality.

Information Security issues to be considered when implementing your policy include the following:

- When leaving a message, you could give confidential information to unauthorised parties.
- When recording a message to be played back to callers, you may inadvertently alert them to your absence or convey confidential information (in an attempt to be 'helpful').

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.5 Security of electronic office systems
8.7.7 Other forms of information exchange

Policy 010708
Taking Equipment off the Premises

SUGGESTED POLICY STATEMENT

"Only authorised personnel are permitted to take equipment belonging to the organisation off the premises; they are responsible for its security at all times."

EXPLANATORY NOTES

When taking organisation equipment off site, once proper authorisation has been obtained, the next key consideration is the physical security of the equipment. A further critical consideration is the security of any information contained on it. Often, the data is far more valuable than the equipment itself.

Information Security issues to be considered when implementing your policy include the following:

- Confidential data may be exposed to unauthorised persons.
- Where no policy and procedures exist regarding the removal of equipment from the premises, items can become 'lost' or 'missing'. Where sensitive information is stored on such equipment, the impact could be considerable.
- Where equipment is not 'signed for' when removed from the premises, its location, expected return and overall security can be compromised.
- Equipment on loan, and in your custody may be lost, stolen or tampered with.
- Equipment may be lent to family or friends for personal use with the possible loss or corruption of data and / or configuration settings.
- Where shared laptops or other PCs have password protected files, this can frustrate use and prevent legitimate access to information.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.5 Security of equipment off-premises
7.3.2 Removal of property

Policy 010709
Maintaining Hardware (On-site or Off-site Support)

SUGGESTED POLICY STATEMENT

"All equipment owned, leased or licensed by the organisation must be supported by appropriate maintenance facilities from qualified engineers."

EXPLANATORY NOTES

The arrangements you make for maintaining your equipment, whether through on-site support or off-site support.

Information Security issues to be considered when implementing your policy include the following:

- Physical access to computers offers the opportunity for disclosure of information to unauthorised individuals.
- Theft or 'disappearance' of hardware incurs unnecessary costs. Malfunction of repaired equipment can cause disruption to data processing.
- Where the supplier's recommended maintenance or service interval is overlooked, both the equipment and any open data files could fail/become corrupted.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.4 Equipment maintenance

Policy 010710
Using Speed Dialling Telephone Options

SUGGESTED POLICY STATEMENT

"All speed dialling systems must incorporate security features which protect sensitive or confidential information."

EXPLANATORY NOTES

Speed dialling facilities create Information Security risks as confidential customer contact information can be accessed just by pressing telephone keys.

Information Security issues to be considered when implementing your policy include the following:

- Sensitive information may be stolen because callers masquerade as you over the telephone.
- Secure or unlisted phone numbers may be acquired from your stored information.
- Secure or unlisted phone numbers may be acquired from global information stored in your *PBX*.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.7 Other forms of information exchange.

Policy 010711
Cleaning of Keyboards and Screens

SUGGESTED POLICY STATEMENT

"Only suitable and approved cleaning materials are to be used on equipment owned by the organisation."

EXPLANATORY NOTES

Cleaning keyboards and screens is a standard housekeeping function and therefore will rarely be queried. However, there are inherent risks such as damage to the machine, and possible risks of information being disclosed to unauthorised parties - perhaps posing as a cleaning crew.

Information Security issues to be considered when implementing your policy include the following:

- Confidential material may be read by unauthorised parties whilst cleaning equipment.
- Loss and damage to equipment due to inappropriate use of cleaning fluid or methods.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.4 Equipment maintenance

Policy 010712
Damage to Equipment

SUGGESTED POLICY STATEMENT

"Deliberate or accidental damage to organisation property must be reported to the nominated Information Security Officer as soon as it is noticed."

EXPLANATORY NOTES

Damage to equipment must be reported as soon as it is discovered. Repair any damaged equipment that affects your Information Security without delay as you could possibly lose valuable items and information through any weak links.

Information Security issues to be considered when implementing your policy include the following:

- Where property, which is a part of your security safeguards, is damaged, it may be an unacceptably weak link, negating strengths in other areas.
- Damage to equipment may be the result of poor training, inappropriate procedures or extreme usage, beyond the supplier's recommended limits. Sudden failure may result.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.4(c) Equipment maintenance
8.4.3 Fault logging

CHAPTER 02
CONTROLLING ACCESS TO INFORMATION AND SYSTEMS

Sub-Chapter 01 Controlling Access to Information and Systems

Sub-Chapter 01
Controlling Access to Information and Systems

Policy 020101
Managing Access Control Standards

SUGGESTED POLICY STATEMENT

"Access control standards for information systems must be established by management and should incorporate the need to balance restrictions to prevent unauthorised access against the need to provide unhindered access to meet business needs."

EXPLANATORY NOTES

Access control standards are the rules which an organisation applies in order to control access to its *information assets*. Such standards should always be appropriate to the organisation's business and security needs. The dangers of using inadequate access control standards range from inconvenience to critical loss or corruption of data.

See also *Data classification* to assess information for its sensitivity levels.

Information Security issues to be considered when implementing your policy include the following:

- The lack of uniform standards controlling the access to information and systems can lead to disparities and weaknesses, which could be exploited for malicious or other reasons.
- Where access control is not modified in response to the enhanced sensitivity of processed information, the risk of a breach to its confidentiality will increase – perhaps substantially.
- Access control standards which are too tight or inflexible can impede the organisation's day-to-day activities and frustrate staff.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.1.1. Access control policy
9.2.4 Review of user access rights
9.5.8 Limitation of connection time

Policy 020102
Managing User Access

SUGGESTED POLICY STATEMENT

"Access to all systems must be authorised by the owner of the system and such access, including the appropriate access rights (or privileges) must be recorded in an Access Control List. Such records are to be regarded as Highly Confidential documents and safeguarded accordingly."

EXPLANATORY NOTES

Good management of user access to information systems allows you to implement tight security controls and to identify breaches of *Access Control* standards.

Information Security issues to be considered when implementing your policy include the following:

- Lack of a managed access control procedure can result in unauthorised access to information systems thereby compromising confidentiality and potentially the integrity of the data.
- Logon screens or banners which supply information about the system prior to successful logon, should be removed as they can assist unauthorised users to gain access. See also Legal Safeguards against Computer Misuse.
- Where regulation and documentation of *Access Control* has been informal, this can frustrate the re-allocation of duties because there are no records of current access rights and privileges.
- Allocating inappropriate privileges to inexperienced staff can result in accidental errors and processing problems.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.2. Access Management

Policy 020103
Securing Unattended Workstations

SUGGESTED POLICY STATEMENT

"Equipment is always to be safeguarded appropriately - especially when left unattended."

EXPLANATORY NOTES

Computer equipment which is logged on and unattended can present a tempting target for unscrupulous staff or third parties on the premises. However, all measures to make it secure should observe your *Access Control* Policy.

Information Security issues to be considered when implementing your policy include the following:

- Unauthorised access of an unattended workstation can result in harmful or fraudulent entries, e.g. modification of data, fraudulent e-mail use, etc.
- Access to an unattended workstation could result in damage to the equipment, deletion of data and / or the modification of system / configuration files.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.3.1. Clear desk and clear screen policy
9.3.2 Unattended user equipment

Policy 020104
Managing Network Access Controls

SUGGESTED POLICY STATEMENT

"Access to the resources on the network must be strictly controlled to prevent unauthorised access. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised."

EXPLANATORY NOTES

Connections to the network (including users' logon) have to be properly managed to ensure that only authorised devices / persons are connected.

Information Security issues to be considered when implementing your policy include the following:

- Unauthorised access to programs or applications could lead to fraudulent transactions or false entries.
- Where physical or *logical access* has not been controlled, users may find (and exploit) unintentional access routes to systems and network resources. For example: they connect a laptop to a disused wall socket, bypass the login server, and connect directly to the main server.
- Unauthorised external access to your network will usually result in damage, corruption and almost certain loss of confidentiality of corporate information. Such hacks are usually motivated by malicious or fraudulent indent.
- Incomplete or incorrect data in a user's network access profile could result in their being permitted to modify, delete, or have access to, confidential information on inappropriate network resources.
- Modifications made to a network access profile without adequate change control procedures in place could result in unexpected (and probably accidental) access to unauthorised network resources. (See above.)
- User IDs which suggest their privileges (e.g. a User ID of '*allprivs*') may invite hackers to try hard to crack their password.
- Connections to a third party network (say, in Business to Business e-Commerce situations), can not only possibly introduce viruses, but can also disrupt business operations where data is inadvertently transmitted into your network.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.4. Network Access Control

Policy 020105
Controlling Access to Operating System Software

SUGGESTED POLICY STATEMENT

"Access to operating system commands is to be restricted to those persons who are authorised to perform systems administration / management functions. Even then, such access must be operated under dual control requiring the specific approval of senior management."

EXPLANATORY NOTES

The operating system controls a computer's operations; 'pre-loaded' with it are commands and utilities which set-up and maintain the computer's environment. All systems, from PCs to large servers, should be *hardened* to remove all unnecessary development tools and utilities prior to delivery to end users .

N.B. This policy primarily concerns access to systems running on mature operating systems such as UNIX®, VMS®, MVS®, OS/400® etc.

Information Security issues to be considered when implementing your policy include the following:

- Staff with access to the '$' prompt or *command line*, could succeed in executing system commands, which could damage and corrupt your system and data files.
- Operating system commands could be used to disable or circumvent access control and audit log facilities, etc.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.5. Operating System Access Control

Policy 020106
Managing Passwords

SUGGESTED POLICY STATEMENT

"The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to best practice guidelines. In particular, passwords shall not be shared with any other person for any reason."

EXPLANATORY NOTES

Most computer systems are accessed by a combination of User ID and Password. This policy discusses the management of passwords from an administrator's perspective.

Techniques for devising effective passwords and their uses are explained in *Choosing Passwords* and *Use and Best Practice*.

Information Security issues to be considered when implementing your policy include the following:

- Password allocation via the System Administrator or other technical staff can compromise *access control*, during which time unauthorised access may take place. This will be an unacceptable risk for highly sensitive systems.
- Passwords that are shared may allow unauthorised access to your information systems.
- Users who need to access multiple systems may keep a hand written note of the different passwords - e.g. in a diary - especially where they are changed frequently. Such insecure records make an easy target for ill-intentioned persons wishing to break into the system.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.2.3 User password management
9.3.1 Password use
9.5.2 Terminal log-on procedures
9.5.3 User identification and authentication
9.5.4 Password management system

Policy 020107
Securing Against Unauthorised Physical Access

SUGGESTED POLICY STATEMENT

"Physical access to high security areas is to be controlled with strong identification and authentication techniques. Staff with authorisation to enter such areas are to be provided with information on the potential security risks involved."

EXPLANATORY NOTES

Personnel who work in, or have access to, high security areas may be put under pressure to reveal access codes or keys, or to breach security by performing unauthorised / illegal tasks, such as copying confidential information. The organisation should provide adequate information regarding, and safeguards to prevent, such eventualities.

Information Security issues to be considered when implementing your policy include the following:

- A member of staff may be threatened or coerced to disclose confidential access codes / procedures or information about the organisation's systems.
- A member of staff may be threatened or coerced outside the work place to disclose confidential access codes / procedures or information about the organisation's systems.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.1.2 Physical entry controls

Policy 020108
Restricting Access

SUGGESTED POLICY STATEMENT

"Access controls are to be set at an appropriate level which minimises information security risks yet also allows the organisation's business activities to be carried without undue hindrance."

EXPLANATORY NOTES

Access to systems and their data must be restricted to ensure that information is denied to unauthorised users.

However, inappropriate restrictions could result in individual users being unable to do their job, and cause delays and errors in legitimate data processing. Similarly, excessive privilege could allow an authorised user to damage information systems and files, causing delays and errors.

Information Security issues to be considered when implementing your policy include the following:

- Excessive systems privileges could allow authorised users to modify (or, more likely, corrupt / destroy) the operating system configuration and business software settings with grave results.
- Lack of access restrictions could :-

  1) Allow staff and third parties to modify documents and other data files.

  2) Risk loss of confidentiality and integrity, and also possible legal action for potential infringements of the *Data Protection Act* or local equivalent. See also *Complying with Legal and Policy Requirements*.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.6.1 Information access restriction

Policy 020109
Monitoring System Access and Use

SUGGESTED POLICY STATEMENT

"Access is to be logged and monitored to identify potential misuse of systems or information."

EXPLANATORY NOTES

System access must be monitored regularly to thwart attempts at unauthorised access and to confirm that access control standards are effective.
For large networks, or where intrusion would have serious consequences, *Intrusion Detection Systems* are used.

Information Security issues to be considered when implementing your policy include the following:

- Without frequent monitoring, it is difficult to assess the effectiveness of your access controls. Unauthorised access can remain undetected, enabling knowledge of this 'security hole' to be passed to persons with possible malicious or fraudulent intent. The consequences can be serious.
- Without hard evidence of a security breach, it is difficult to take disciplinary action, and it may be impossible to take legal action, say under the *Computer Misuse Act*. See Legal Safeguards against Computer Misuse.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.7.2 Monitoring system use

Policy 020110
Giving Access to Files and Documents

SUGGESTED POLICY STATEMENT

"Access to information and documents is to be carefully controlled, ensuring that only authorised personnel may have access to sensitive information."

EXPLANATORY NOTES

Controlling access is the way to protect your information and data files.

Information Security issues to be considered when implementing your policy include the following:

- With poor or inadequate access control over your documents and files, information may be copied or modified by unauthorised persons, or become corrupted unintentionally or maliciously.
- Where the *access control* is seen as overly restrictive, users could be tempted to share privileged accounts (login + password) in order to access information.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.2.4 Review of user access rights

Policy 020111
Managing Higher Risk System Access

SUGGESTED POLICY STATEMENT

"Access controls for highly sensitive information or high risk systems are to be set in accordance with the value and classification of the information assets being protected."

EXPLANATORY NOTES

High risk systems require more stringent access control safeguards due to the confidentiality of the information they process and / or the purpose of the system e.g. the funds transfer systems used by banks. Ideally, the operating systems for such systems should be hardened to further enhance security.

Information Security issues to be considered when implementing your policy include the following:

- Access to a critical system from a workstation external to its designated business area can threaten its integrity and safety.
- Access control – both physical and logical should be measurably higher than for other systems.
- Dual control and segregation of duties should be considered for all functions.
- Privileges should be reduced to the lowest level to reasonably perform the job concerned.
- Personnel should be carefully selected with their records vetted for suitability for such jobs.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.6.2 Sensitive system isolation

Policy 020112
Controlling Remote User Access

SUGGESTED POLICY STATEMENT

"Remote access control procedures must provide adequate safeguards through robust identification, authentication and encryption techniques."

EXPLANATORY NOTES

Remote users, either tele-workers or personnel on business trips etc., may need to communicate directly with their organisations' systems to receive / send data and updates.

Such users are physically remote, and they will often be connecting through public (insecure) networks. This increases the threat of unauthorised access.

Information Security issues to be considered when implementing your policy include the following:

- The use of a User ID and password as the sole means of *access control*, may provide inadequate security to enable access to the organisation's systems - especially where telephone dial up access is permitted.
- Remote access may be denied to authorised users leading both to a denial of service and also an alert that access control may have been compromised internally.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.4.3 User authentication for external connections

CHAPTER 03
PROCESSING INFORMATION AND DOCUMENTS

Sub-Chapter
01 Networks

Policy 030101 **Configuring Networks**

Policy 030102 **Managing the Network**

Policy 030103 **Accessing your Network Remotely**

Policy 030104 **Defending your Network Information from Malicious Attack**

Policy 030101
Configuring Networks

SUGGESTED POLICY STATEMENT

"The network must be designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and a range of privilege restrictions."

EXPLANATORY NOTES

The configuration of your network impacts directly on its performance and affects its stability and Information Security.

Information Security issues to be considered when implementing your policy include the following:

- Poor network stability can threaten your business operations.
- Inadequate control over access to your network can jeopardise the confidentiality and integrity of your data.
- Slow or inadequate system response times impede business processing.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.5 Network Controls
9.4 Network access control
9.4.1 Policy on use of network services

Policy 030102
Managing the Network

SUGGESTED POLICY STATEMENT

"Suitably qualified staff are to manage the organisation's network, and preserve its integrity in collaboration with the nominated individual system owners."

EXPLANATORY NOTES

All but the smallest networks, where changes are relatively infrequent, require ongoing management.

Information Security issues to be considered when implementing your policy include the following:

- Inappropriate control over access to the network will threaten the confidentiality and integrity of your data.
- Inadequate capacity can make efficient operation difficult or impossible.
- Slow or inadequate system response times impedes business processing.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1 Security in job definition and resourcing
8.5.1 Network controls
9.4.1(c) Policy on use of network services

Policy 030103
Accessing your Network Remotely

SUGGESTED POLICY STATEMENT

"Remote access to the organisation's network and resources will only be permitted providing that authorised users are authenticated, data is encrypted across the network, and privileges are restricted."

EXPLANATORY NOTES

The means by which your information systems network may be accessed from an external source. Remote access was traditionally provided by means of dial-up or leased phone lines. Today however, the *Virtual Private Network* provides access across public networks, e.g. the Internet.

Information Security issues to be considered when implementing your policy include the following:

- Inadequate Internet Security safeguards can allow unauthorised access to your network, with potentially disastrous consequences.
- Weak dial-in security standards can give unauthorised access to your network, the consequences of which could be very serious.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.4.3 User authentication for external connections

Policy 030104
Defending your Network Information from Malicious Attack

SUGGESTED POLICY STATEMENT

"System hardware, operating and application software, the networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised network intrusion."

EXPLANATORY NOTES

The measures taken to defend your computer hardware against physical damage, and your software from unauthorised usage.

Information Security issues to be considered when implementing your policy include the following:

- Your hardware can be physically damaged, through a malicious act, perhaps necessitating a system close down or delayed operations.
- Unauthorised and inappropriate use of your software can lead to malicious and / or fraudulent amendment of your records.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.3.1 Controls against malicious software

Sub-Chapter 02
System Operations and Administration

Policy 030201
Appointing System Administrators

SUGGESTED POLICY STATEMENT

"The organisation's systems are to be managed by a suitably qualified systems administrator who is responsible for overseeing the day to day running and security of the systems."

EXPLANATORY NOTES

The System Administrator is responsible for overseeing the day-to-day running of a computer system. This usually entails ensuring that the computer system is available and appropriately configured to perform required tasks, rather than 'hands-on' production. System administration necessarily involves a substantial amount of security-related work. In larger organisations this function can be undertaken by a separate *Security Administrator*, who is part of the Security Officer's team.

Information Security issues to be considered when implementing your policy include the following:

- A System Administrator who lacks the relevant knowledge, experience, and training may make errors which cost the organisation dearly.
- The high degree of discretion inherent in the System Administrator's job in itself poses a security threat.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.3 Allocation of information security responsibilities

Policy 030202
Administrating Systems

SUGGESTED POLICY STATEMENT

"System Administrators must be fully trained and have adequate experience in the wide range of systems and platforms used by the organisation. In addition, they must be knowledgeable and conversant with the range of Information Security risks which need to be managed."

EXPLANATORY NOTES

A System Administrator is often in a powerful position because they normally set the user access criteria for all systems. This raises a range of Information Security issues. The System Administrator must receive an adequate level of training on the system within their area of responsibility. The System Administrator must also be familiar with the Information Security risks associated with the system administration function.

Information Security issues to be considered when implementing your policy include the following:

- Any system or network changes implemented by the System Administrator are likely to be far-reaching; errors can threaten the entire network's operation.
- Running both live systems and test / development systems on the same computer is extremely dangerous because a program crash on the test system could impact the live (production) environment.
- Employees with a grievance pose a serious risk because they know what information of value exists and they may be able to circumvent security controls.
- Where users' access rights and privileges are not documented, Information Security may be compromised.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.3 Allocation of information security responsibilities

Policy 030203
Controlling Data Distribution

SUGGESTED POLICY STATEMENT

"For authorised personnel, the appropriate data and information must be made available as and when required; for all other persons, access to such data and information is prohibited with appropriate technical control required to supplement the enforcement of this policy."

EXPLANATORY NOTES

Ensuring that your organisation's data and information are neither divulged nor accessible to unauthorised persons.

Information Security issues to be considered when implementing your policy include the following:

- Sensitive information, not classified as such, is at risk of being divulged inappropriately.
- The practice of making multiple copies of an original file (e.g. because several people need it) may jeopardise its reliability and integrity and cast doubt on the validity of all associated and subsequent work. Longer term, this reflects poorly on the integrity of your organisation as a whole.
- Staff who are frustrated because they cannot access data relevant to their jobs may be tempted to convey this frustration to your customers. This can damage your business.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.1 Business requirement for access control

Policy 030204
Permitting Third Party Access

SUGGESTED POLICY STATEMENT

"Third party access to corporate information is only permitted where the information in question has been 'ring fenced' and the risk of possible unauthorised access is considered to be negligible."

EXPLANATORY NOTES

Allowing persons external to your organisation access to your systems and data.

Information Security issues to be considered when implementing your policy include the following:

- Permitting access by a third party can not only compromise the confidentiality of your information, but can also result in loss of data validity and integrity. All threats associated with remote access apply here also.
- Ambiguous or inappropriate data may be released to third parties, resulting in possible confusion and / or reduced business confidence in your organisation and its products / services.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.2.1 Identification of risks from third party access

Policy 030205
Managing Electronic Keys

SUGGESTED POLICY STATEMENT

"The management of electronic keys to control both the encryption and decryption of sensitive messages must be performed under dual control, with duties being rotated between staff."

EXPLANATORY NOTES

Electronic keys are used to encrypt and de-crypt messages sent between one or more parties. Usually such cryptographic techniques will be used where the transmission circuits are across non secure lines. The management of the electronic keys is a critical aspect of implementing a *Public Key Infrastructure* solution.

Information Security issues to be considered when implementing your policy include the following:

- If your private key becomes compromised, invalid messages could be sent which forge the authentication of your organisation. Such security breaches could result in substantial fraud.
- If you fail to manage the keys of the various senders of encrypted data, you may fail to decrypt an incoming message, with potential costly delays.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.3.1 Policy on the use of cryptographic controls
10.3.5 Key management

Policy 030206
Managing System Operations and System Administration

SUGGESTED POLICY STATEMENT

"The organisation's systems must be operated and administered using documented procedures in a manner which is both efficient but also effective in protecting the organisation's information security."

EXPLANATORY NOTES

The means by which your IT systems are run and maintained on a day-to-day basis.

Information Security issues to be considered when implementing your policy include the following:

- A failure to establish robust and appropriately scheduled routines can lead to poor reliability and systems disruption.
- All systems are likely to experience periodic problems which must be handled appropriately, or a relatively minor problem could escalate into a major incident.
- Operational shortcuts can lead to processing errors and reduce effectiveness of safeguards.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.4.1 Control of operational software
8.4.2 Operator logs

Policy 030207
Managing System Documentation

SUGGESTED POLICY STATEMENT

"System documentation is a requirement for all the organisation's information systems. Such documentation must be kept up-to-date and be available."

EXPLANATORY NOTES

The management of the documentation provided for the operation and maintenance of your systems.

Information Security issues to be considered when implementing your policy include the following:

- Missing or inadequate technical documentation, especially with older 'in house' systems, will usually result in operational difficulties and substantially increased system's analysis effort. In such cases:

    1) You are likely to be totally dependent on a few key staff.

    2) You cannot validate proposed technical changes.

    3) You have no effective way to train support staff.

- Out-of-date documentation can result in severe operational or maintenance difficulties.
- If documentation is 'merely' inaccessible, the purchase or development of replacement documentation is unlikely to be a priority. However, the risks are similar to having missing or inadequate documentation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.4 Security of system documentation
10.5.1 (h) Change control procedures

Policy 030208
Monitoring Error Logs

SUGGESTED POLICY STATEMENT

"Error logs must be properly reviewed and managed by qualified staff."

EXPLANATORY NOTES

Error logs are the reports produced by your system relating to errors or inconsistencies that have arisen during processing are important sources of information for ensuring proper use of the system.

Information Security issues to be considered when implementing your policy include the following:

- Error log entries may be concealed, due to attempted system intrusion / break in, or someone trying to 'cover their tracks', possibly after a series of errors arising from negligence.
- A failure to review error logs regularly from each production system can jeopardise the safe and efficient running of your systems.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.7.1 Event logging
9.7.2 Monitoring system use

Policy 030209
Scheduling Systems Operations

SUGGESTED POLICY STATEMENT

"Systems Operations schedules are to be formally planned, authorised and documented."

EXPLANATORY NOTES

Whilst many systems appear to 'run themselves' e.g. the Web server or the file server, many systems require a combination of routine maintenance and also processing 'runs' or 'batch jobs'. Especially where *interfaces* have been developed which require the export from one system to become the import to another system, detailed scheduling is required, to avoid processing 'snarl ups'

Information Security issues to be considered when implementing your policy include the following:

- If *jobs* are not planned and scheduled properly, updates and processing may fail or only partially complete.
- Unauthorised / Unscheduled system processing can result in errors, failure and / or fraud.
- Resource contention can cause delays or errors in your processing.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.1.1 Documented operating procedures

Policy 030210
Scheduling Changes to Routine Systems Operations

SUGGESTED POLICY STATEMENT

"Changes to routine systems operations are to be fully tested and approved before being implemented."

EXPLANATORY NOTES

Alterations that require changes to your routine computer systems operations introduce risk. Such changes are likely to be necessitated by enhancements to your hardware or software, or may simply be a reflection of revised schedules, possibly called for by your users.

Information Security issues to be considered when implementing your policy include the following:

- Any change to your Systems Operations Schedule introduces risk. The outcome can be anything from a minor error, to a failed job with all those jobs reliant upon it potentially also failing.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.1.2 Operational change control

Policy 030211
Monitoring Operational Audit Logs

SUGGESTED POLICY STATEMENT

"Operational audit logs are to be reviewed regularly by trained staff and discrepancies reported to the owner of the information system."

EXPLANATORY NOTES

The files written by your system(s) containing details of the changes made to your records, and to your operational environment, require close monitoring.

Information Security issues to be considered when implementing your policy include the following:

- Audit Logs may be inoperative or 'de-selected', in order to conceal present or future unauthorised systems activities.
- Accidental loss of Audit Logs removes your audit trail, and hence the possible inability to determine the source of a problem.
- Audit logs may not be taken seriously by Systems Operations staff or other operational staff, and may not be reviewed regularly.
- Audit logs may not be viewed by staff who understand the significance of the error messages.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.4.2 Operator logs
12.3.1 System audit controls

Policy 030212
Synchronising System Clocks

SUGGESTED POLICY STATEMENT

"System clocks must be synchronised regularly especially between the organisation's various processing platforms."

EXPLANATORY NOTES

The need to ensure that where the time related information is held within your systems, it is adjusted for your own time zone. Most computer clocks tend to vary in their accuracy, but this should not be significant. However, if these differences become material, then this may have security implications for your organisation, especially where transaction timing is crucial.

Information Security issues to be considered when implementing your policy include the following:

- If there is a significant difference between system time and actual time your computer's scheduled tasks may malfunction.
- Manipulating 'system time' may enable fraud to be perpetrated.
- The *integrity* of *Error* and *Audit Logs* with significant 'time stamp' errors can invalidate the contents of the log. This can be crucial when investigating security incidents on your system(s). See *Collecting Evidence of an Information Security Breach*.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.7.3 Clock synchronisation

Policy 030213
Responding to System Faults

SUGGESTED POLICY STATEMENT

"Only qualified and authorised staff or approved third party technicians may repair information system hardware faults."

EXPLANATORY NOTES

Responding to problems that may impact on your system, making accurate and timely processing difficult. See also *Recording and Reporting Hardware Faults*.

Information Security issues to be considered when implementing your policy include the following:

- Naïve, but well intentioned attempts to solve an apparently 'simple' problem can inadvertently magnify it so that information access or processing is restricted or totally prevented.
- Resolving the problem can take longer, and can be more complex than anticipated, delaying processing and on-line information access throughout the organisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.4.3 Fault logging

Policy 030214
Managing or Using Transaction / Processing Reports

SUGGESTED POLICY STATEMENT

"Transaction and processing reports should be regularly reviewed by properly trained and qualified staff."

EXPLANATORY NOTES

The primary systems of your organisation, e.g. the accounting system and transaction processing systems, should each allow the production of a frequent report, usually daily, which shows the entries processed for the period in question. Such reports should be either printed automatically, or be available 'on line'.

Information Security issues to be considered when implementing your policy include the following:

- Lack of, or low priority, procedures for agreeing transaction logs will increase the opportunity for undetected entries and fraud.
- Unauthorised amendment to the Transaction Processing Reports could conceal a fraud.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.2.2 Control of internal processing

Policy 030215
Commissioning Facilities Management - FM

SUGGESTED POLICY STATEMENT

"Any Facilities Management company must be able to demonstrate compliance with this organisation's Information Security Policies and also provide a Service Level Agreement which documents the performance expected and the remedies available in case of non compliance."

EXPLANATORY NOTES

The commissioning of an outside organisation to run your IT systems.

Information Security issues to be considered when implementing your policy include the following:

- Poor or inadequate service delivered by the FM company can result in disruption to your business operations.
- The risk of compromise to the confidentiality of sensitive information is heightened by outsourcing.
- Inadequate provisions for compliance with legal or statutory requirements, e.g. Data Protection, can jeopardise the integrity of your business operations.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.3 Outsourcing

Sub-Chapter 03
E-mail and the Worldwide Web

Policy 030301
Downloading Files and Information from the Internet

SUGGESTED POLICY STATEMENT

"Great care must be taken when downloading information and files from the Internet to safeguard against both malicious code and also inappropriate material."

EXPLANATORY NOTES

There are significant Information Security risks when you download any files (including graphics files of any format), programs, or scripts, etc from the Internet.

Information Security issues to be considered when implementing your policy include the following:

- In the process of downloading *applications* (programs) from the Internet to your PC, you may receive a *virus* or other *malicious code* which infects your system. This can have extremely serious consequences.
- Downloaded software is likely to require licensing or you run the risk of legal action from the supplier. See *Software Licensing*.
- Information on the Internet may be inaccurate, invalid, or deliberately misleading, and any decisions based upon it must be subject to close scrutiny.
- Abuse of your organisation's Internet access can overload your network and increase the risk of systems failure due to *contention*.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.3.1(b) Controls against malicious software
9.1.1 Access control policy

Policy 030302
Using and Receiving Digital Signatures

SUGGESTED POLICY STATEMENT

"The transmission of sensitive and confidential data is to be authenticated by the use of digital signatures whenever possible."

EXPLANATORY NOTES

The option of using *Digital Signatures* in electronic mail used over the Internet, provides a means of introducing a high degree of security to an otherwise insecure medium.

Information Security issues to be considered when implementing your policy include the following:

- An e-mail with important contents, and 'signed' with a Digital Signature may still not be acted upon by the recipient, resulting in possible delays and loss to your organisation.
- Important electronic mail communications may not be authenticated and can result in unauthorised instructions being issued.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.3.3 Digital signatures

Policy 030303
Sending Electronic Mail (E-mail)

SUGGESTED POLICY STATEMENT

"E-mail should only be used for business purposes, using terms which are consistent with other forms of business communication. The attachment of data files to an e-mail is only permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code."

EXPLANATORY NOTES

The use of e-mail has escalated to the point where it is obligatory for all companies to be accessible through this medium. The inherent lack of security for sending messages, information, files or instructions appears to be ignored by many, who see the benefits of near instant, and virtually free, global communications as far outweighing any possible 'downside'.

Sending e-mail using a *Digital Signature* (and optionally being encrypted), is a means of ensuring its validity and *integrity* to the recipient. The content of e-mails received without such authentication may be considered unreliable.

Information Security issues to be considered when implementing your policy include the following:

- The transmission of a virus can not only damage the recipient's system but can permanently damage your organisation's reputation.
- Sending e-mail via insecure public lines (e.g. the Internet) can compromise the Confidentiality and Integrity of the information being transmitted. It is similar to a post card because any one who picks it up is able to read it.
- Confidential files may be transmitted by e-mail as attachments thus breaching confidentiality and potentially leading to financial loss.
- Relying upon e-mail from a legal perspective, is not advised, as simple e-mail messages are not usually authenticated.
- Personal e-mail sent from one individual to another through the organisation's systems, can be misconstrued as coming from the organisation and can result in Information Security issues.
- Correspondence sent from an individual's personal mail box could possibly be regarded as personal, thus preventing the organisation from inspecting / reviewing it.
- Sending a copy of files to colleagues on your internal network, creates unnecessary duplicates and also compromises the integrity of the original document / file.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.3.4 Non-repudiation services
8.7.4 Security of electronic mail
10.2.3 Message authentication

Policy 030304
Receiving Electronic Mail (E-mail)

SUGGESTED POLICY STATEMENT

"Incoming e-mail must be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code."

EXPLANATORY NOTES

The use of e-mail has escalated to the point where it is obligatory for all companies to be accessible by e-mail. The inherent lack of security for receiving messages, information, files or instructions appears to be ignored by many, who see the benefits of near instant, and virtually free, global communications as far out weighing any 'downside'.

Receiving e-mail using a Digital Signature (and optionally being encrypted), is a means of ensuring its validity and *integrity*. The content of e-mails received without such authentication may be unreliable.

Information Security issues to be considered when implementing your policy include the following:

- The receipt, failure to detect, and the introduction of a virus, can not only damage your own system and data, but can also spread throughout the organisation's network, wreaking havoc.
- Placing legal reliance upon an e-mail is dangerous, as simple e-mail messages cannot be authenticated.
- Receiving e-mail via unsecured public lines (e.g. the Internet) can compromise the confidentiality and integrity of the contents.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.3.1(b) Controls against malicious software
10.2.3 Message authentication

Policy 030305
Retaining or Deleting Electronic Mail

SUGGESTED POLICY STATEMENT

"Data retention periods for e-mail must be established to meet legal and business requirements and must be adhered to by all staff."

EXPLANATORY NOTES

Whereas the filing of printed business correspondence is often performed centrally, the management of e-mail 'boxes' is often performed individually or by group. However, because simple e-mail has little legal significance for the purpose of contractual commitment (See *Digital Signatures*) it may not be clear what e-mail correspondence should be retained.

Information Security issues to be considered when implementing your policy include the following:

- Retention of all e-mail can consume significant storage capacity on your system; especially where files have been sent / received.
- Accidental deletion of important messages can result in problems and duplication of work.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.3 Safeguarding of organisational records

Policy 030306
Setting up Intranet Access

SUGGESTED POLICY STATEMENT

"Persons responsible for setting up Intranet access must ensure that any access restrictions pertaining to the data in source systems, are also applied to access from the organisation's Intranet."

EXPLANATORY NOTES

An intranet is a Web based information service that is available only **within** your organisation and its internal network(s).

The use of an intranet raises many of the security issues associated with the Internet, in that your intranet could permit unauthorised access to information which should not be made available generally. The key security issue therefore is one of *confidentiality* through *access control*.

Information Security issues to be considered when implementing your policy include the following:

- Inadequate security measures can lead to the disclosure of sensitive data to unauthorised persons; either via the organisation's public Web site; its 'restricted access' *Extranet* or by direct connection using 'hacking' techniques.
- Access to the intranet may allow unauthorised persons within the organisation to view sensitive data, thereby compromising internal confidentiality.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.1.1 Access control policy

Policy 030307
Setting up Extranet Access

SUGGESTED POLICY STATEMENT

"Persons responsible for setting up Extranet access must ensure that any access restrictions pertaining to the data in source systems, are also applied to access from the organisation's Extranet".

EXPLANATORY NOTES

An Extranet is a semi-private Web site and extends beyond an organisation's internal network. Typically it permits access to selected organisational data from clients, suppliers, or third parties using a User ID, password and, optionally (for greater security) *Digital Certificates*.

Information Security issues to be considered when implementing your policy include the following:

- Inadequate security measures can lead to the disclosure of sensitive data to unauthorised persons.
- Duplication of information for publication on an extranet can result in a loss of integrity between the source and the copy.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.1.1 Access control policy

Policy 030308
Setting up Internet Access

SUGGESTED POLICY STATEMENT

"Persons responsible for setting up Internet access are to ensure that the organisation's network is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall. Human Resources management must ensure that all personnel with Internet access (including e-mail) are aware of, and will comply with, an acceptable code of conduct in their usage of the Internet in addition to compliance with the organisation's Information Security Policies."

EXPLANATORY NOTES

Accessing the Internet raises a wide range of Information Security issues.

The dangers arising from downloading information from the Internet are addressed in *Downloading Files and Information from the Internet*. The potential threats raised in respect of sending and receiving e-mails are considered in *Sending Electronic Mail* and *Receiving Electronic Mail*. The need to have formalised procedures for dealing with electronic message storage and deletion is dealt with in *Retaining or Deleting Electronic Mail*.

Information Security issues to be considered when implementing your policy include the following:

- Full time connection to the Internet offers unrivalled opportunities for opportunistic / malicious infiltration from hackers who can 'see' your *IP Address* on the network and are then able to probe its 'weak spots'.
- Where staff are permitted access the Internet for non business purposes, this may result in contention for resources, reduced performance and lowered efficiency.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.1.1 Access control policy

Policy 030309
Developing a Web Site

SUGGESTED POLICY STATEMENT

"Due to the significant risk of malicious intrusion from unauthorised external persons, Web sites may only be developed and maintained by properly qualified and authorised personnel."

EXPLANATORY NOTES

There are many potential Information Security dangers that you should be aware of when you develop an Internet web site.

Information Security issues to be considered when implementing your policy include the following:

- Access to the corporate (internal network) via the Web server can result in exposure of information to unauthorised persons who may have criminal intentions.
- Opportunistic and pre-meditated intrusion can result in the corruption of the Web site including defamatory messages and the theft / destruction of its data files.
- Confidential data can be revealed to unauthorised persons which may lead to loss, embarrassment and / or damage to the organisation.
- The capture of logon details through line tapping and / or 'sniffers' can result in an attempted intrusion.
- Information posted on your Web site may be copied and reproduced without elementary copyright notices.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.3 Electronic commerce security

Policy 030310
Receiving Misdirected Information by E-mail

SUGGESTED POLICY STATEMENT

"Unsolicited e-mail is to be treated with caution and not responded to."

EXPLANATORY NOTES

You should never bother to reply to unsolicited e-mails as this could tell the sender who may be a potential hacker that the address is real and is being read by a real person, and thereby could possibly open the door to a virus or denial of service attack.

Information Security issues to be considered when implementing your policy include the following:

- Receiving unsolicited or 'spam' e-mail may overload the system and drain resources.
- An automatic 'Return Receipt' may be generated from unsolicited or misdirected e-mail confirming to the sender that you have opened their e-mail.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.4 Security of electronic mail

Policy 030311
Forwarding E-mail

SUGGESTED POLICY STATEMENT

"Ensure that information you are forwarding by e-mail (especially attachments) is correctly addressed and only being sent to appropriate persons."

EXPLANATORY NOTES

When you forward an e-mail to someone else you are adding your name and details to it. Ensure you are comfortable with the information contained in the original. Any security risk associated with the original mail to you will also apply to the forwarded e-mail.

Information Security issues to be considered when implementing your policy include the following:

- Sending a virus in forwarded e-mail may result in data loss and systems' corruption for the recipient which could then lead to possible legal action and financial liability.
- Forwarding an incorrect file attachment may release confidential information.
- Inappropriate / unauthorised material being attached may cause embarrassment or even financial loss to your organisation.
- Forwarding e-mail to an incorrect address may result in data being lost or stolen and, at the very least, a loss of confidentiality.
- Forwarding large files (over 1MB) to multiple recipients may congest their networks or mail systems.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.4 Security of electronic mail

Policy 030312
Using Internet for Work Purposes

SUGGESTED POLICY STATEMENT

"Management is responsible for controlling user access to the Internet, as well as for ensuring that users are aware of the threats, and trained in the safeguards, to reduce the risk of Information Security incidents."

EXPLANATORY NOTES

The use of the Internet is now becoming widespread at work and consumes significant employee resource in terms of time spent 'on-line'. An appropriate policy needs to be set to avoid unnecessary time spent on the Internet.

Information Security issues to be considered when implementing your policy include the following:

- Unauthorised and un-guarded use of the facilities on the Internet, may offer hackers the opportunity to access to your information and systems.
- Unauthorised purchases are made via the Internet.
- The visited Web site will often record your details to facilitate navigation and choices upon re-visiting the site. However such capture and storage of information is often without your knowledge.
- Inappropriate access and downloads can be considered both a misuse of the organisation's resources and, in some cases, can be illegal.
- Unauthorised use of the Internet wastes time and resources.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.1.1 Access control policy

Policy 030313
Giving Information when Ordering Goods on Internet

SUGGESTED POLICY STATEMENT

"Staff authorised to make payment by credit card for goods ordered on the Internet, are responsible for its safe and appropriate use."

EXPLANATORY NOTES

The use of a credit or debit card to purchase goods on the Internet is becoming widespread, with an increased risk of theft and potential security breaches.

Information Security issues to be considered when implementing your policy include the following:

- Confidential organisation credit card details (PIN numbers & account details) may be compromised during transmission.
- Passing credit card details to unknown third parties on the Internet compromises security.
- Lost or stolen credit card numbers may be posted and used on the Internet.
- Where the security safeguards of the organisation running the Web server are in doubt, any confidential information posted to their Web site may be maliciously or inadvertently exposed.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.3 Electronic commerce security
8.7.6 Publicly available systems

Policy 030314
'Out of the Box' Web Browser Issues

SUGGESTED POLICY STATEMENT

"Web browsers are to be used in a secure manner by making use of the built-in security features of the software concerned. Management must ensure that staff are made aware of the appropriate settings for the software concerned."

EXPLANATORY NOTES

Web browser software and e-mail software are new paths through an organisation's security shield which could be exploited by an intruder. The security issues are in the areas of *Cookies*, Java applets, JavaScript, ActiveX controls and *viruses*. The use of a *firewall* may be unable to protect you from attack via *malicious code* activated by your web browser.

Information Security issues to be considered when implementing your policy include the following:

- Where viruses, Trojan applications and *malicious code* are able to penetrate your defences and activated by your Web browser, serious damage may result.
- Confidential data may be stored and accessed through a *cookie* saved on your PC and accessed by a Web site whilst you are browsing - likely without your knowledge.
- Staff may not be aware of the necessary settings and related policy for ensuring security when using web browsers.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.3 Electronic commerce security
8.7.6 Publicly available systems

Policy 030315
Using Internet 'Search Engines'

SUGGESTED POLICY STATEMENT

"Information obtained from Internet sources should be verified before used for business purposes."

EXPLANATORY NOTES

The Internet has become a vast source of knowledge. However, the integrity of information sourced from the Internet must be verified.

Information Security issues to be considered when implementing your policy include the following:

- Where downloaded information is used in a calculation or in making an important decision without verifying the information, embarrassment and loss may result when the data is found to be inaccurate or totally wrong.
- If information obtained from the Internet is not verified, then decisions made which depend upon that information may be incorrect. There is a substantial amount of misinformation on the Internet

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.3 Electronic commerce security

Policy 030316
Maintaining your Web Site

SUGGESTED POLICY STATEMENT

"The Web site is an important marketing and information resource for the organisation, and its safety from unauthorised intrusion is a top priority. Only qualified authorised persons may amend the Web site with all changes being documented and reviewed."

EXPLANATORY NOTES

Information on your Web site, whether being hosted by an *ISP* or in-house, must be kept up to date and secure, even during periods of Web site maintenance.

Information Security issues to be considered when implementing your policy include the following:

- Where hosting a Web site in-house, opportunistic hackers may attempt to gain unauthorised access to data within your organisation's main computer network.
- During Web site maintenance data may be more vulnerable to theft or destruction.
- Data may stolen or modified whilst the security feature of your Web site are disabled for maintenance, especially when working on the security features themselves.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.3 Electronic commerce security

Policy 030317
Filtering Inappropriate Material from the Internet

SUGGESTED POLICY STATEMENT

"The organisation will use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet by staff. Reports of attempted access will be scrutinised by management on a regular basis."

EXPLANATORY NOTES

Many organisations with in-house IT capability are now placing restrictive filters which prevent access by employees through the internet to sites displaying inappropriate material.

Information Security issues to be considered when implementing your policy include the following:

- Employees may accidentally or deliberately access and download inappropriate material from the Internet, causing possible concern and distress to themselves or other employees.
- Inappropriate and even illegal information may be accessed and downloaded where the filtering mechanisms are inadequate or not kept up to date.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.1.1 Access control policy

Policy 030318
Certainty of File Origin

SUGGESTED POLICY STATEMENT

"Computer files received from unknown senders are to be deleted without being opened."

EXPLANATORY NOTES

It is vital that the information you receive is complete and correct. Take care with hard copy information and electronically supplied data in case of possibility of forgery.

Information Security issues to be considered when implementing your policy include the following:

- Malicious software could have been sent from a suspect information source.
- Decisions could be taken based upon the assumed authenticity of an expected report or file.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.3.1 Controls against malicious software

Sub-Chapter 04
Telephones & Fax

Policy 030401
Making Conference Calls

SUGGESTED POLICY STATEMENT

"Conference calls are only permitted if staff are aware of the Information Security issues involved."

EXPLANATORY NOTES

Using the telephone to provide simultaneous discussions between three or more persons. The threats posed by Conference Calls are similar to those posed by conventional person-to-person calls.

Information Security issues to be considered when implementing your policy include the following:

- An overheard or (worse) tapped conversation can result in leaked information. Where the information is sensitive, is potentially very damaging.
- Failing to authenticate the identity of other parties to the conversation can result in a breach to information confidentiality.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.5 Security of electronic office systems
8.7.7 Other forms of information exchange

Policy 030402
Using Video Conferencing Facilities

SUGGESTED POLICY STATEMENT

"Video conference calls are only permitted if staff are aware of the Information Security issues involved."

EXPLANATORY NOTES

Using communication network facilities to provide simultaneous sound and vision facilities between individuals or groups of individuals.

Information Security issues to be considered when implementing your policy include the following:

- An overheard or (worse) tapped meeting can result in leaked information. Where such information is sensitive, the results can potentially be very damaging.
- Failing to authenticate the identity of other parties to the video conference can result in a breach to information confidentiality.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.5 Security of electronic office systems
8.7.7 Other forms of information exchange

Policy 030403
Recording of Telephone Conversations

SUGGESTED POLICY STATEMENT

"All parties are to be notified in advance whenever telephone conversations are to be recorded."

EXPLANATORY NOTES

Recording telephone calls is generally carried out either to provide an authoritative source in the event of disputed details, or to monitor the adequacy of telephone responses being given to customers calling-in by telephone.

Information Security issues to be considered when implementing your policy include the following:

- Failure to observe the terms of relevant legislation can result in your organisation becoming liable to prosecution.
- A failure to inform the recorded party that calls are recorded can prevent / hinder the use of such recordings when and if, needed.
- Accidental loss of recorded media, can result in the non-availability of a vital recording with consequent damage and / or frustration to your organisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.5 Security of electronic office systems
8.7.7 Other forms of information exchange

Policy 030404
Receiving Misdirected Information by Fax

SUGGESTED POLICY STATEMENT

"Any fax received in error is to be returned to the sender. Its contents must not be disclosed to other parties without the sender's permission."

EXPLANATORY NOTES

Information received in a misdirected fax should be treated as highly confidential and should not be divulged to others.

Information Security issues to be considered when implementing your policy include the following:

- A misdirected fax can be received from either external or internal sources, and needs to be treated as a sensitive document.
- Staff may not be aware of the requirement to return misdirected faxes, and may not treat the contents in an appropriate manner.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.5 Security of electronic office systems
8.7.7 Other forms of information exchange

Policy 030405
Giving Information when Ordering Goods on Telephone

SUGGESTED POLICY STATEMENT

"Staff authorised to make payment by credit card for goods ordered over the telephone, are responsible for safe and appropriate use."

EXPLANATORY NOTES

If confidential information is required when ordering goods on the telephone it is necessary to ensure that you know exactly to whom you are talking and whether they are authorised to handle such information.

Information Security issues to be considered when implementing your policy include the following:

- Confidential organisation credit card details (PIN numbers & account details) may be compromised.
- Credit cards may be easily lost or stolen.
- Where credit card users are also those who authorise the payments, a conflict of interest may arise which compromises your spending control.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.5 Security of electronic office systems
8.7.7 Other forms of information exchange

Policy 030406
Persons Giving Instructions over the Telephone

SUGGESTED POLICY STATEMENT

"The identity of recipients of sensitive or confidential information over the telephone must be verified."

EXPLANATORY NOTES

It is not uncommon for instructions or information to be given over the telephone, but this raises the issue of verifying the identity of the caller. Be aware of *social engineering* where the aim is to trick people into revealing passwords or other information that compromises a target system's security

Information Security issues to be considered when implementing your policy include the following:

- Risk of passing on personal data.
- Risk of passing organisation data to unauthorised parties.
- Callers may gain information by deception, e.g. claiming to be a person who is entitled access to confidential information.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.5 Security of electronic office systems
8.7.7 Other forms of information exchange

Policy 030407
Persons Requesting Information over the Telephone

SUGGESTED POLICY STATEMENT

"The identity of persons requesting sensitive or confidential information over the telephone must be verified, and they must be authorised to receive it."

EXPLANATORY NOTES

Callers to your organisation may claim to be someone who is entitled to access confidential material. Be aware of *social engineering*.

Information Security issues to be considered when implementing your policy include the following:

- Callers may claim to be someone who is entitled access to confidential information and gain information by deception.
- Risk of passing personal data.
- Risk of passing organisation data to unauthorised parties.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.5 Security of electronic office systems
8.7.7 Other forms of information exchange

Policy 030408
Receiving Unsolicited Faxes

SUGGESTED POLICY STATEMENT

"Unsolicited or unexpected faxes should be treated with care until the sender has been identified."

EXPLANATORY NOTES

Unsolicited faxes are common. Much of it is junk advertising material and should be ignored. Be on your guard against possible 'probing'.

Information Security issues to be considered when implementing your policy include the following:

- Faxes which 'look official' can lead to the disclosure of confidential information.
- Responding to unsolicited faxes may encourage further faxes from the same source. This could be part of a plan by an opportunist hacker probing your area for information bites to find security holes.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.5 Security of electronic office systems
8.7.7 Other forms of information exchange

Sub-Chapter 05
Data Management

Policy 030520 Using and Deleting 'Temp' Files

Policy 030521 Using Customer and Other Third Party Data Files

Policy 030522 Saving Data / Information by Individual Users

Policy 030501
Transferring and Exchanging Data

SUGGESTED POLICY STATEMENT

"Sensitive or confidential data / information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured e.g. by using encryption techniques."

EXPLANATORY NOTES

The way in which your data is distributed across networks (both public and private) and by other means e.g. the exchange of tapes, disks, diskettes and optical disks (e.g. CD-ROMs).

Information Security issues to be considered when implementing your policy include the following:

- Incorrect data released to outside parties can lead to a loss of confidence in the organisation and / or its services.
- Any illegal amendment of / tampering with your data whilst in transit suggests a weakness that is being exploited by techno-criminals / hackers.
- Where security measures have not been adequately deployed, sensitive information may be accessed by unauthorised persons.
- Confidential data may be distributed to inappropriate / unauthorised persons.
- The recipient of your data may have adopted Information Security standards which are incompatible with yours. This constitutes a weak link in your security which could be exploited.
- The inappropriate and possibly illegal release of information may result in legal action and prosecution.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.7 Other forms of information exchange

Policy 030502
Managing Data Storage

SUGGESTED POLICY STATEMENT

"Day-to-day data storage must ensure that current data is readily available to authorised users and that archives are both created and accessible in case of need."

EXPLANATORY NOTES

The storage of information and data is a day to day function for all organisations. It requires careful management to ensure that Information Security issues are dealt with adequately

Information Security issues to be considered when implementing your policy include the following:

- Where data and information files are not saved and stored securely, your organisation's activities can be severely disrupted.
- Important data may become unavailable due to deletion. This can lead to a range of difficulties, the least of which may be embarrassment.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.3 Information handling procedures
12.1.3 Safeguarding of organisational records

Policy 030503
Managing Databases

SUGGESTED POLICY STATEMENT

"The integrity and stability of the organisation's databases must be maintained at all times."

EXPLANATORY NOTES

The majority of your organisation's data, such as client records, accounting data, project information, sales, and purchases, are likely to be held in databases of some form. Some databases will require active management, e.g. 'relational databases' which comprise multiple tables of data.

Information Security issues to be considered when implementing your policy include the following:

- A failure to manage the technical requirements of the database can result in a failure of the database itself and the applications which access and update it.
- Unless the data is periodically cleansed, its integrity will diminish as duplications and ambiguous records persist.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.2. Security in application systems
12.1.3 Safeguarding of organisational records

Policy 030504
Permitting Emergency Data Amendment

SUGGESTED POLICY STATEMENT

"Emergency data amendments may only be used in extreme circumstances and only in accordance with emergency amendment procedures."

EXPLANATORY NOTES

Sometimes referred to as 'data surgery', these measures are adopted when live data must be altered by other than normal software functions and procedures. This can occur when, for example, 'the system' will not permit the change to a data field on a 'confirmed' transaction - and yet the data is incorrect. Such manipulation of data is dangerous and can have knock-on effects, but occasionally it is necessary. Proceed with extreme caution.

Information Security issues to be considered when implementing your policy include the following:

- Emergency data amendment can bypass your normal controls with the consequent scope for fraud and error.
- Unless rigorous procedures are implemented to control emergency data amendments, files may become corrupted or manipulated.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.5.1 Change control procedures

Policy 030505
Receiving Information on Disks

SUGGESTED POLICY STATEMENT

"The use of removable media disks e.g. disks and CD-ROMs is not permitted except where specifically authorised."

EXPLANATORY NOTES

Disks and CD-ROMs are easily transportable and are the primary means of data distribution. Their contents can often be read at most workstations and, once copied onto the corporate network, the origin may be untraceable.

Information Security issues to be considered when implementing your policy include the following:

- Seemingly innocent documents can conceal a virus or other *malicious code*, potentially causing damage and disruption.
- Old versions of documents and other files may overwrite newer versions, possibly destroying valuable work.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.3.1 Controls against malicious software

Policy 030506
Setting up a New Folder / Directory

SUGGESTED POLICY STATEMENT

"Data directories and structures should be established by the owner of the information system with users adhering to that structure. Access restrictions to such directories should be applied as necessary to restrict unauthorised access."

EXPLANATORY NOTES

Controlling access to your data is best done at the network access level. Directory structures on a stand-alone machine should be intuitive to prevent accidental deletion, and the whole machine should have a power-on password with sensitive files given individual passwords.

Information Security issues to be considered when implementing your policy include the following:

- Inappropriate access to the directory can expose your files to unauthorised users.
- Data can be difficult (or impossible) to locate as a result of badly named directories.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.1.1 Access control policy

Policy 030507
Amending Directory Structures

SUGGESTED POLICY STATEMENT

"Existing directory and folder structures may only be amended with the appropriate authorisation, usually from the owner of the information system concerned."

EXPLANATORY NOTES

The directory structure is a route map for the storage and access to files and data. Any unauthorised changes to data paths may cause access rights to be circumvented.

Information Security issues to be considered when implementing your policy include the following:

- Directory / files may be deleted accidentally.
- Where data seems to be missing with a warning message (e.g. 'Document or file name not valid') when trying to re-open a document or file, it could indicate that the file has been moved, deleted or modified without your knowledge.
- Files can be difficult to locate because the file *path* itself may have been changed without your knowledge.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.1.1 Access control policy

Policy 030508
Archiving Documents

SUGGESTED POLICY STATEMENT

"The archiving of documents must take place with due consideration for legal, regulatory and business issues with liaison between technical and business staff."

EXPLANATORY NOTES

You may wish to archive documents for various reasons, such as: lack of space in the live system, removal of old data that has been processed at the end of a pre-defined period (end of the month or year), or legal requirements to retain the information. The policy for archiving should be set by the department that is responsible for determining organisation records policy.

Information Security issues to be considered when implementing your policy include the following:

- Not having a Retention Policy may lead to data or files being deleted inappropriately resulting in both embarrassment and possibly legal action.
- Despite being on remote store, information files can be lost or stolen.
- Document control problems may make the recovery of information impossible.
- Documents 'cannot be found' leading to frustration and possible loss.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.3 Safeguarding of organisational records

Policy 030509
Information Retention Policy

SUGGESTED POLICY STATEMENT

"The information created and stored by the organisation's information systems must be retained for a minimum period that meets both legal and business requirements."

EXPLANATORY NOTES

This section relates to retaining information other than documents or files.

Information Security issues to be considered when implementing your policy include the following:

- Information could be lost or destroyed if no retention policy is defined, resulting in both embarrassment and possibly legal action.
- Once defined, the retention policy needs to be enforced to avoid incorrect retention periods being applied to documents and records.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.3 Safeguarding of organisational records

Policy 030510
Setting up New Spreadsheets

SUGGESTED POLICY STATEMENT

"The classification of spreadsheets must be appropriate to the sensitivity and confidentiality of data contained therein. All financial / data models used for decision making are to be fully documented and controlled by the information owner. "

EXPLANATORY NOTES

Spreadsheets are mainly used for accounting, financial modelling, or as a key tool in a scenario modelling exercise. They may even be used as a 'flat file' data base.

Information Security issues to be considered when implementing your policy include the following:

- Unless the formulae are validated, decisions may be based upon false numbers.
- New spreadsheets may be set up without proper consideration as to their data content, and the appropriate storage and *access control* to apply to the data.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.2.2 System acceptance
10.5.1 Change control procedures

Policy 030511
Setting up New Databases

SUGGESTED POLICY STATEMENT

"Databases must be fully tested for both business logic and processing, prior to operational usage. Where such databases are to contain information of a personal nature, procedures and access controls must ensure compliance with necessary legislation e.g. Data Protection."

EXPLANATORY NOTES

Databases are set-up so that specific data can be stored, retrieved and reorganised. This makes the maintenance of security and integrity of the data particularly important.

Information Security issues to be considered when implementing your policy include the following:

- Without a careful and diligent testing of a database, its processing and reporting may be false, which could lead to inappropriate business decisions.
- New databases may be set up without proper consideration as to their data content and the appropriate storage and *access control* to apply to the data.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.2.2 System acceptance
10.5.1 Change control procedures

Policy 030512
Linking Information between Documents and Files

SUGGESTED POLICY STATEMENT

"Highly sensitive or critical documents must not rely upon the availability or integrity of (external) data files over which the author may have no control. Key documents and reports must be self contained and contain all the necessary information."

EXPLANATORY NOTES

Linking documents is a way of transferring and/or sharing data between documents or programs. For example, the monthly sales report written using a word processor, may take the figures directly from an embedded link to the sales spreadsheet which itself has a link to the Order Processing System.

Information Security issues to be considered when implementing your policy include the following:

- Linked data within your document may become modified without your knowledge or consent, damaging the integrity of the contents of your document.
- Where your document does not reflect changes to the source data, its integrity is lost and readers could be mis-led.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.3 Information handling procedures

Policy 030513
Updating Draft Reports

SUGGESTED POLICY STATEMENT

"Draft reports should only be updated with the authority of the designated owner of the report."

EXPLANATORY NOTES

The updating of draft reports should always be authorised by the document owner. Draft documents should be clearly labelled as such.

Information Security issues to be considered when implementing your policy include the following:

- Sensitive information is included in a draft document but the document is inappropriately handled leading to loss of confidentiality.
- A draft document is thought to be final and is signed off in error, leading to confusion and embarrassment.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.2.2 Information labelling and handling
9.1.1 Access control policy

Policy 030514
Deleting Draft Reports

SUGGESTED POLICY STATEMENT

"Draft version(s) of reports must be deleted or archived following production of a final version. A single version of the file should be retained for normal operational access."

EXPLANATORY NOTES

Earlier draft versions of reports should be deleted or archived to prevent further use of the document and its information.

Information Security issues to be considered when implementing your policy include the following:

- Unauthorised access to classified information may be possible from obsolete copies of draft reports.
- Draft reports, if not deleted, may contain incorrect information which could result in inappropriate decisions being made where management have access to these draft reports.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.2.2 Information labelling and handling
9.1.1 Access control policy

Policy 030515
Using Version Control Systems

SUGGESTED POLICY STATEMENT

"Version control procedures should always be applied to documentation belonging to the organisation or its customers."

EXPLANATORY NOTES

Version control systems are normally an integral part of a document management system. They advise the status of documents and provide a control over their secure distribution.

Information Security issues to be considered when implementing your policy include the following:

- Sensitive information may be excluded from the document management procedures / system and be exposed to possible unauthorised access.
- Inappropriate decisions may be made, based upon an earlier version of a document

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.5.1 Change control procedures

Policy 030516
Sharing Data on Project Management Systems

SUGGESTED POLICY STATEMENT

"Only authorised persons may access sensitive or confidential data on projects owned or managed by the organisation or its employees."

EXPLANATORY NOTES

Project management systems range from simple handwritten lists, spreadsheets or documents to sophisticated Project Management software. Due to the nature of project work, in its early stages, much information is sensitive and even secret. As project phases are completed the sensitivity of the information may be downgraded and the information may then become public knowledge.

Information Security issues to be considered when implementing your policy include the following:

- If information relating to internal projects is accessed by unauthorised persons, the organisation's plans and objectives can become exposed to both unauthorised persons internally and also to external parties. Such disclosure can have serious impact upon an organisation's market valuation (share price), public and employee relations.
- Sensitive or classified organisation data may be released along with unclassified data.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.1.1 Access control policy

Policy 030517
Updating Customer Information

SUGGESTED POLICY STATEMENT

"Customer information may only be updated by authorised personnel. Customer data is to be safeguarded using a combination of technical access controls and robust procedures, with all changes supported by journals and internal audit controls."

EXPLANATORY NOTES

Customer information held by the organisation needs regular updates, including additions, modifications, and archiving. At all such times, confidentiality must be maintained.

Information Security issues to be considered when implementing your policy include the following:

- Where customer information is unavailable due to an incorrect update or other inaccuracy, all records pertaining to that customer may become corrupted, causing potential loss and even legal infringement.
- Confidential customer data supplied may be incorrect, either intentionally or in error.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.4 Data protection and privacy of personal information

Policy 030518
Using Meaningful File Names

SUGGESTED POLICY STATEMENT

"The naming of the organisation's data files must be meaningful and capable of being recognised by its intended users."

EXPLANATORY NOTES

The naming of files is often arbitrary and therefore results in unintended confusion. Standards and naming conventions should be established.

Information Security issues to be considered when implementing your policy include the following:

- Meaningless or non-standard file names can result in data becoming lost or hard to find.
- Staff must be required to comply with standards for naming data files and data structures.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.2.2 Information labelling and handling

Policy 030519
Using Headers and Footers

SUGGESTED POLICY STATEMENT

"A document's security classification level and ownership should be stated within the header and footer space on each page of all documents."

EXPLANATORY NOTES

All pages should at a minimum have headers and footers which display their classification level and ownership copyright.

Information Security issues to be considered when implementing your policy include the following:

- The classification of a document is not displayed thereby risking possible inadvertent exposure to unauthorised persons.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.2.1 Classification guidelines
5.2.2 Information labelling and handling

Policy 030520
Using and Deleting 'Temp' Files

SUGGESTED POLICY STATEMENT

"Temporary files on users' PCs and laptops are to be deleted regularly to prevent possible misuse by possible unauthorised users."

EXPLANATORY NOTES

Computer systems often use temporary files as a way to simplify the management of data you are working with, e.g. temporary back ups and fast saves, clip board files, printer files etc.

Information Security issues to be considered when implementing your policy include the following:

- If your PC's operating system or a software program *crashes*, 'temp' files may be left behind which could disclose confidential information to unauthorised persons

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.4 Housekeeping

Policy 030521
Using Customer and Other Third Party Data Files

SUGGESTED POLICY STATEMENT

"Customer contact information is to be classified as Highly Confidential and secured accordingly."

EXPLANATORY NOTES

Customer and other contact address files could be important information to your competitors. They should be considered as sensitive material and secured accordingly.

Information Security issues to be considered when implementing your policy include the following:

- The theft of customer and contact information is not only the potential loss of a *business asset* it may also contravene the law.
- Where contact information is incorrect or 'dated' you may inadvertently send confidential information which may then be stolen with any confidentiality lost.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1 Compliance with legal requirements

Policy 030522
Saving Data / Information by Individual Users

SUGGESTED POLICY STATEMENT

"All users of information systems whose job function requires them to create or amend data files, must save their work on the system regularly in accordance with best practice, to prevent corruption or loss through system or power malfunction."

EXPLANATORY NOTES

The saving of data in a structured and timely manner is good practice for all users of workstations and terminals.

Information Security issues to be considered when implementing your policy include the following:

- Overwriting data files using the same file name will destroy any previous file; which could lead to problems in the event that the new version is incorrect or possibly corrupted.
- Failing to save data can result in the loss of work in the event of a system *crash*.
- Saving data in an incorrect folder or disk can frustrate colleagues and can lead to the use of 'old' or incorrect data in error.
- Saving data on a local workstation disk (e.g. the 'C drive') may appear more convenient but it can frustrate access by colleagues and probably will not be backed up.
- Saving data on your 'system disk' (e.g. the 'C' drive) is particularly risky as any requirement to upgrade / replace the operating system would likely destroy the data files (unless you remembered to back them up!)

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.2.2 Information labelling and handling

Sub-Chapter 06
Backup, Recovery and Archiving

Policy 030601
Restarting or Recovering your System

SUGGESTED POLICY STATEMENT

"Information system owners must ensure that adequate back up and system recovery procedures are in place."

EXPLANATORY NOTES

The facilities employed to ensure that your computer processing re-starts successfully after a voluntary or enforced close down.

Information Security issues to be considered when implementing your policy include the following:

- The unavailability of your systems (and data) following an interruption to normal processing can impact on business operations and efficiency.
- Corruption / loss of some data following an interruption to normal processing can disrupt operations and delay business processing.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.4.1 Information back-up

Policy 030602
Backing up Data on Portable Computers

SUGGESTED POLICY STATEMENT

"Information and data stored on Laptop or portable computers must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis."

EXPLANATORY NOTES

Backing up data held on portable computing devices is a means to protect against loss.

Information Security issues to be considered when implementing your policy include the following:

- Data held on a laptop computer may be lost, due to an internal (system) failure; such data may be of significant value - especially to the individual concerned.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.8.1 Mobile computing

Policy 030603
Managing Backup and Recovery Procedures

SUGGESTED POLICY STATEMENT

"Backup of the organisation's data files and the ability to recover such data is a top priority. Management are responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business."

EXPLANATORY NOTES

The need for, and creation of, end of day backup files cannot be over emphasised as they allow you to restore either the whole system or perhaps selected data files, to a specified 'end of day' position. However, the procedures used to initiate such a 'recovery' must be clearly documented and tested - the Information Security implication of an inappropriate or incorrect file restore, are significant.

Information Security issues to be considered when implementing your policy include the following:

If restore procedures have not been tested, a partial or invalid restore can corrupt the entire system, which may partly or extensively terminate business operations

- Where backup procedures are inadequate or lacking, data may be lost or, effectively, unavailable, this compromising the organisation's business processes.
- Opportunistic or malicious modification of the daily backup sequence results in a failure to safeguard all required data.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.4.1 Information back-up

Policy 030604
Archiving Information

SUGGESTED POLICY STATEMENT

"The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered, especially where proprietary formats are involved."

EXPLANATORY NOTES

This refers to information which is not required on a day to day basis, but which needs to be retained for a certain period, and also information which is retained in perpetuity and referred to infrequently but periodically. Such data is often removed from your day-to-day processing, thereby reducing the *overhead* on storage and processing resources.

Information Security issues to be considered when implementing your policy include the following:

- Weaknesses in the longevity of the media used for archives can result in a failure to restore the required data when, eventually, it is needed.
- Archived data can often be retained in a proprietary format which is no longer supported by your present systems, thus frustrating attempts at access.

  N.B. This is a real risk that has yet to be fully quantified. With the accelerating evolution of operating systems, processor technology, and applications software, it is uncertain which of the late 20th century and early 21st century 'standards', will still be in use say in 10 years time, when the need arises to restore the data files from pre-2000.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.4.1 Information back-up

Policy 030605
Archiving Electronic Files

SUGGESTED POLICY STATEMENT

"The archiving of electronic data files must reflect the needs of the business and also any legal and regulatory requirements."

EXPLANATORY NOTES

Archiving electronic files follows the same guidelines as archiving documents, but covers additional information about retrieval.

Information Security issues to be considered when implementing your policy include the following:

- Not having a suitable Retention Policy could lead to data being deleted inappropriately.
- Where legacy documents 'cannot be found' they may have been inappropriately deleted or prematurely archived.
- Information can be lost whilst storing confidential items off site.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.4.1 Information back-up

Policy 030606
Recovery and Restoring of Data Files

SUGGESTED POLICY STATEMENT

"Management must ensure that safeguards are in place to protect the integrity of data files during the recovery and restoration of data files; especially where such files may replace more recent files."

EXPLANATORY NOTES

Saving of data on a backup tape or disc is a core process in the security of your information.

Information Security issues to be considered when implementing your policy include the following:

- Data could be accessed and restored by unauthorised parties using similar backup software.
- The required data, when restored, is not on the designated backup tape or disc resulting in confusion and potential loss.
- The required data, whilst located and restored, is found to be corrupt.
- Data may be lost or overwritten by the incorrect restoration from back up media.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.4.1 Information back-up

Sub-Chapter 07
Document Handling

Policy 030701
Managing Hard Copy Printouts

SUGGESTED POLICY STATEMENT

"Hard copies of sensitive or classified material must be protected and handled according to the distribution and authorisation levels specified for those documents."

EXPLANATORY NOTES

Managing and controlling the hard-copy reports produced by your computer programs.

N.B. The guidance provided in this section is aimed primarily at paper-based reports, however similar guidelines also apply to other forms of non-electronic output, such as microfiche.

Information Security issues to be considered when implementing your policy include the following:

- Sensitive documented information material may be routed to office printers where confidentiality may be lost; or at the least, threatened.
- Secure filing systems are to be used for sensitive documents and reports in order to avoid access by unauthorised persons.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.3 Information handling procedures

Policy 030702
Photocopying Confidential Information

SUGGESTED POLICY STATEMENT

"All employees to be aware of the risk of breaching confidentiality associated with the photocopying (duplication) of sensitive documents. Authorisation from the document owner should be obtained where documents are classified as Highly Confidential or above."

EXPLANATORY NOTES

Photocopy machines are located in almost every office in the world. Often located in public areas they are simple to use and almost everyone has occasion to do so as a legitimate part of their job. This makes spotting fraudulent use all the more difficult.

Information Security issues to be considered when implementing your policy include the following:

- Unauthorised copies can be made releasing confidential information.
- Authorised copies may be mislaid, disclosing confidential information to unauthorised parties.
- Unauthorised persons can nevertheless sometimes gain access to sensitive material and use copying facilities for personal or other reasons.
- Unauthorised people may see and remove copies during the copy / binding process.
- Unauthorised people may see the contents of the document during copying.
- Confidentiality can be breached by original sheets being left in machine.
- Sheets of partially copied material can become jammed in the machine which can disclose sensitive information to unauthorised persons e.g. the person removing the blockage.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.3 Information handling procedures

Policy 030703
Filing of Documents and Information

SUGGESTED POLICY STATEMENT

"All information used for, or by the organisation, must be filed appropriately and according to its classification."

EXPLANATORY NOTES

Secure filing and storage of sensitive material is essential to guard against loss and unauthorised access.

Information Security issues to be considered when implementing your policy include the following:

- Important information may be lost or stolen because files have been misplaced or lost.
- Informal document filing procedures could result in theft of information.
- In the event of fire, flood or other disaster, documents may be destroyed.
- Where sensitive information is not handled appropriately, it could be seen by unauthorised persons.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.3 Information handling procedures

Policy 030704
The Countersigning of Documents

SUGGESTED POLICY STATEMENT

"Documents should be countersigned (either manually or electronically) to confirm their validity and integrity; especially those which commit or oblige the organisation in its business activities."

EXPLANATORY NOTES

A sign off process is intended to ensure that the transaction or document has been properly checked and authorised. Normally, the person applying the second signatory or initial will take prime responsibility.

Information Security issues to be considered when implementing your policy include the following:

- If transactions are not verified for correctness, there is a high risk of loss through mistake or theft.
- Organisation resources may be stolen or misappropriated if there is no accountability for information correctness.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.3 Information handling procedures

Policy 030705
Checking Document Correctness

SUGGESTED POLICY STATEMENT

"Documents should be checked to confirm their validity and integrity; especially those which commit or oblige the organisation in its business activities."

EXPLANATORY NOTES

Sound decision making relies on having the correct information available. With most security breaches being the result of internal errors checking documents for correctness becomes a high priority.

Information Security issues to be considered when implementing your policy include the following:

- If documents are not reviewed for correctness this may result in incorrect decisions being made and possibly cause financial loss.
- Unverified information may be unreliable.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.3 Information handling procedures

Policy 030706
Approving Documents

SUGGESTED POLICY STATEMENT

"All written communications sent out by the organisation to third parties are to be approved by authorised persons."

EXPLANATORY NOTES

The authorisation of documents is fundamental to their acceptance and credibility.

Information Security issues to be considered when implementing your policy include the following:

- Unauthorised documents could be acted upon resulting in financial loss.
- Documents are to be authorised strictly in accordance with the organisation's authorised signatory policy and procedures.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.3 Information handling procedures

Policy 030707
Verifying Signatures

SUGGESTED POLICY STATEMENT

"All signatures authorising access to systems or release of information must be properly authenticated."

EXPLANATORY NOTES

It is critical to establish the signatory's authenticity and level of authority. This topic deals with physical signatures. Digital /electronic signatures are covered elsewhere.

Information Security issues to be considered when implementing your policy include the following:

- Data or information may be stolen by using an unauthenticated signature.
- Where the signatory is not authorised to approve a particular transaction or activity, financial loss may result.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.3 Information handling procedures

Policy 030708
Receiving Unsolicited Mail

SUGGESTED POLICY STATEMENT

"Unsolicited mail should not receive serious attention until and unless the sender's identity and authenticity of the mail have been verified."

EXPLANATORY NOTES

Unsolicited mail may simply be misaddressed, and therefore returning it to sender may be all that is required. However, you should be aware that unsolicited physical and electronic mails may be used to probe your security systems and to gain unauthorised information.

Information Security issues to be considered when implementing your policy include the following:

- You may unintentionally disclose additional sensitive information when returning mail to the original sender.
- Information is disclosed in response to letters or memos which look official.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.3 Information handling procedures

Policy 030709
Style and Presentation of Reports

SUGGESTED POLICY STATEMENT

"An agreed 'corporate' document style should be used which promotes consistency, integrity and promotes the agreed 'image' of the organisation."

EXPLANATORY NOTES

The risks to organisation information are made greater when you do not maintain organisation document standards. These standards for documentation presentation and report structures should give the author a framework to write reports and the audience a way to quickly absorb the correct message or information.

Information Security issues to be considered when implementing your policy include the following:

- Where non standard presentation styles are used, this may result in confused messages and possibly conflicting statements.
- Style standards and templates are to be developed and implemented in order to ensure standardisation across the organisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.3 Information handling procedures

Policy 030710
Transporting Sensitive Documents

SUGGESTED POLICY STATEMENT

"The designated owners of documents which contain sensitive information are responsible for ensuring that the measures taken to protect their confidentiality, integrity and availability, during and after transportation / transmission, are adequate and appropriate."

EXPLANATORY NOTES

When selecting the most suitable delivery option for your documents it is important to pay strict attention to the information classification level and to any security risk to the information, such as mishandling and misuse, and also to the potential for theft inherent in each delivery option, delivery media and delivery location.

Information Security issues to be considered when implementing your policy include the following:

- If the transport medium is inappropriate for the sensitivity / value of the information being transported, it could facilitate the theft of the contents whilst in transit.
- If the transport medium used does not protect confidential data, or does not protect from transit damage, information may be lost or at least delayed.
- Electronic transport methods may expose or damage confidential data in transit.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.2.2 Information labelling and handling
8.7.2 Security of media in transit

Policy 030711
Shredding of Unwanted Hardcopy

SUGGESTED POLICY STATEMENT

"All documents of a sensitive or confidential nature are to be shredded when no longer required. The document owner must authorise or initiate this destruction."

EXPLANATORY NOTES

All organisations print documents and reports. Unwanted hardcopy, especially confidential or controlled copies, should be disposed of securely. The data owner is the only person allowed to authorise document destruction. It is common practice to shred sensitive material.

Information Security issues to be considered when implementing your policy include the following:

- Unintentional leaking of sensitive information from discarded confidential material.
- If third party secure disposal firms are used, ensure that their procedures conform to your expectations.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.2 Disposal of media

Policy 030712
Using Good Document Management Practice

SUGGESTED POLICY STATEMENT

"All users of information systems must manage the creation, storage, amendment, copying and deletion / destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. The degree to which software techniques and disciplined user procedures are necessary will be applied by management and determined by the classification of the information / data in question."

EXPLANATORY NOTES

The integrity of the information held in documents is compromised if the status of the document itself is in doubt.

Information Security issues to be considered when implementing your policy include the following:

- Confusion may arise between different versions of a document, e.g. because there may be multiple copies, none of which is the authoritative version.
- Documents that should be retained may be accidentally lost or simply destroyed / deleted in error.
- Authenticity may be in question because of possible manipulation of text in electronic documents.
- The context of documents may be lost, e.g. because related documents are not linked or kept together.
- Documents may become inaccessible because of technological change, e.g. changes in software or storage media making the files unreadable.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.3 Information handling procedures

Sub-Chapter 08
Securing Data

Policy 030801
Using Encryption Techniques

SUGGESTED POLICY STATEMENT

"Where appropriate, sensitive or confidential information or data should always be transmitted in encrypted form. Prior to transmission, consideration must always be given to the procedures to be used between the sending and recipient parties and any possible legal issues from using encryption techniques."

EXPLANATORY NOTES

Encrypting or scrambling data to assure confidentiality and integrity.

Information Security issues to be considered when implementing your policy include the following:

- Weak administration and procedures surrounding the all-important *encryption keys* can limit the effectiveness of this security measure.
- Encrypted information may be secure, but it may also prove to be inaccessible, even to authorised persons, where keys are poorly managed.
- Processor capacity *(overhead)*is used by the process of *encryption* and *decryption*. Lack of available capacity could lead to the data being effectively 'unavailable' when actually needed.
- In some countries, it is illegal to use *ciphers*; or the type of permissible cipher may be strongly regulated. This could result in unintentionally breaking the law where encrypted data is sent to such a country.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.2.1 Classification guidelines
10.3.2 Encryption
12.1.6 Regulation of cryptographic controls

Policy 030802
Sharing Information

SUGGESTED POLICY STATEMENT

"Persons responsible for Human Resources Management are to ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the organisation and to external parties."

EXPLANATORY NOTES

Sharing information between different divisions, groups or sections of your organisation is often necessary for the business or organisation to function. This raises Information Security issues.

Information Security issues to be considered when implementing your policy include the following:

- Confidential data that is not protected from, or released to, unauthorised parties is a fundamental Information Security failure which can lead to prosecution where the organisation's management has failed to execute its duty of care.
- The inappropriate and possibly unlawful release of information may result in legal liability and prosecution.
- Release of certain data, even if inadvertently, to other parts of your organisation may contravene legal and / or other regulations, and could lead to prosecution or other penalties.
- The recipient of the information, or the recipient's systems, may jeopardise the confidentiality of sensitive documents and data, thereby becoming a security threat which could be exploited.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.2.1 Classification guidelines
12.1.4 Data protection and privacy of personal information

Policy 030803
Sending Information to Third Parties

SUGGESTED POLICY STATEMENT

"Prior to sending information to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and Information Security measures adopted by the third party, must be seen to continue to assure the confidentiality and integrity of the information."

EXPLANATORY NOTES

When sending information to external third parties the principal consideration should be the integrity and confidentiality of the data.

Information Security issues to be considered when implementing your policy include the following:

- Third parties receiving the data may not treat it in a confidential manner, resulting in the data being accessed by unauthorised persons.
- Information security procedures at the offices of the recipient may be inadequate.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.1 Information and software exchange agreements

Policy 030804
Maintaining Customer Information Confidentiality

SUGGESTED POLICY STATEMENT

"Information relating to the clients and third party contacts of the organisation is confidential, and must be protected and safeguarded from unauthorised access and disclosure."

EXPLANATORY NOTES

Keeping customer information confidential is both a legal requirement and essential for organisational credibility.

Information Security issues to be considered when implementing your policy include the following:

- The confidentiality of personal customer data may be compromised if it is given to an unauthorised third party.
- The confidentiality of data may be compromised if requests by unauthorised persons are acceded to.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.4 Data protection and privacy of personal information

Policy 030805
Handling of Customer Credit Card Details

SUGGESTED POLICY STATEMENT

"Customer credit card details entrusted to the organisation must be afforded a combination of security measures (technology and procedural) which, in combination, prevent all recognised possibilities of the card details being accessed, stolen, modified or an any other way divulged to unauthorised persons."

EXPLANATORY NOTES

The use of credit and debit cards has become a major means of making small purchases; especially in the retail / personal sector of Business to Consumer *e-Commerce*. However, with their ease of use, comes a significant security challenge, both for the card holder, the card issuer (who usually indemnifies the card holder against fraud), and the merchant accepting the card.

Information Security issues to be considered when implementing your policy include the following:

- The theft of clients' credit card details jeopardises not only your organisation's reputation with clients and the Card Issuers, but also places the card holders at financial risk.
- Where clients' credit card details are not kept secure, there is a real risk of disclosure to unauthorised persons.
- Disclosure of clients' credit card details to anyone who is not explicitly authorised, jeopardises not only your organisation's reputation with clients and the Card Issuers, but also places the card holders at financial risk.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.3 Electronic commerce security
12.1.4 Data protection and privacy of personal information

Policy 030806
Fire Risks to Your Information

SUGGESTED POLICY STATEMENT

"All data and information must be protected against the risk of fire damage at all times. The level of such protection must always reflect the risk of fire and the value and classification of the information being safeguarded."

EXPLANATORY NOTES

Fire is one of the worst non technology risks you may face. It can cause significant structural damage to your systems.

Information Security issues to be considered when implementing your policy include the following:

- The security of information may be forgotten when a fire evacuation is ordered for the building.
- Although the safety of employees and other persons on the premises must remain paramount, adequate procedures should be in place concerning the security of valuables and information.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.1 Equipment siting and protection

Policy 030807
Sending Out Reports

SUGGESTED POLICY STATEMENT

"Prior to sending reports to third parties, not only must the intended recipient(s) be authorised to receive such information, but the procedures and Information Security measures adopted by each third party, must be seen to continue to assure the confidentiality and integrity of the information."

EXPLANATORY NOTES

When sending out reports be sure that you maintain the confidentiality, and integrity of any data contained therein.

Information Security issues to be considered when implementing your policy include the following:

- Sensitive information may be made available to unauthorised individuals. Reports may be leaked.
- Sensitive information may be included in incorrectly classified reports.
- Sensitive information in reports whether sent electronically or by paper, could be intercepted.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.1 Information and software exchange agreements

Policy 030808
Dealing with Sensitive Financial Information

SUGGESTED POLICY STATEMENT

"Sensitive financial information is to be classified as Highly Confidential and must be afforded security measures (technology and procedural) which, in combination, safeguard such information from authorised access and disclosure."

EXPLANATORY NOTES

Financial information is usually sensitive, especially in competitive markets.

Information Security issues to be considered when implementing your policy include the following:

- Sensitive financial information could be lost or stolen.
- Sensitive financial information may be given to unauthorised parties unintentionally.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.2.1 Classification guidelines

Policy 030809
Deleting Data Created / Owned by Others

SUGGESTED POLICY STATEMENT

"Data is to be protected against unauthorised or accidental changes, and may only be deleted with the proper authority."

EXPLANATORY NOTES

With today's technology it is simple to share information with many people, both intentionally and unintentionally. This raises the problem of data ownership and data custodians, i.e. who is entitled to modify and delete specific data.

Good document management and access control will go a long way to protecting the integrity of your data. Deleting data is a valid house keeping function of the data owners themselves, however, it is wise to back up all such data beforehand.

Information Security issues to be considered when implementing your policy include the following:

- Data and information files may be deleted by unauthorised person, e.g. ill intentioned staff, contractors or even hackers.
- Data may be mistakenly deleted or lost by either technical or business personnel who are manipulating and viewing the data.
- Shared data may be accidentally deleted in error.
- Data may not be available when required.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.1.1 Access control policy

Policy 030810
Protecting Documents with Passwords

SUGGESTED POLICY STATEMENT

"Sensitive / confidential electronic data and information should be secured, whenever possible, with access control applied to the directory on the (computer) system concerned. The sole use of passwords to secure individual documents is less effective, and hence discouraged, as passwords may be either forgotten or become revealed (over time) to unauthorised persons."

EXPLANATORY NOTES

The simplest way to limit access by unauthorised people to your documentation is to apply a password. You may however forget your password and then encounter problems accessing your data.

Information Security issues to be considered when implementing your policy include the following:

- Opening a document or spreadsheet may be impossible where the password has been forgotten or the owner is no longer available.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.1.1 Access control policy

Policy 030811
Printing of Classified Documents

SUGGESTED POLICY STATEMENT

"Information classified as Highly Confidential or Top Secret, may never be sent to a network printer without there being an authorised person to retrieve it and hence safeguard its confidentiality during and after printing."

EXPLANATORY NOTES

Classified documents should have their printing 'rules' included in the master document. All confidential documents should not be unnecessarily copied or have extra copies printed.

Information Security issues to be considered when implementing your policy include the following:

- Confidential data is accessed by unauthorised parties using unofficial/unapproved printed copies.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.3.1 Clear desk and clear screen policy

Sub-Chapter 09
Other Information Handling and Processing

Policy 030901
Using Dual Input Controls

SUGGESTED POLICY STATEMENT

"The decision whether dual control is required for data entry is to be made by the information system owner. Where so required, secure data handling procedures including dual input are to be strictly adhered to."

EXPLANATORY NOTES

Establishing and using a means of verifying and / or validating data by inputting it a second time to a system, and having the results compared to ensure consistency. Such features are often found where the validation of a financial entry is critical, e.g. a payment system.

Information Security issues to be considered when implementing your policy include the following:

- Fraudulent data, input to your system, can result in loss for the organisation.
- Dual control systems should be implemented whenever there is a high risk of loss through single level controls.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.1.4 Segregation of duties

Policy 030902
Loading Personal Screen Savers

SUGGESTED POLICY STATEMENT

"Employees are not permitted to load non-approved screen savers onto the organisation's PCs, laptops and workstations."

EXPLANATORY NOTES

Screen savers are small computer programs which reduce or eliminate 'screen burn' and often provide some visual entertainment or interest.

Information Security issues to be considered when implementing your policy include the following:

- Screen savers can include viruses and other malicious code resulting in local, and potentially, network wide damage.
- Highly graphical (sound and video) screen savers can impact on your systems' resources both by using a relatively large amount of disk storage space and by requiring a significant memory and processor power.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.3.1 Controls against malicious software

Policy 030903
Using External Disposal Firms

SUGGESTED POLICY STATEMENT

"Any third party used for external disposal of the organisation's obsolete equipment and material must be able to demonstrate compliance with this organisation's Information Security Policies and also, where appropriate, provide a Service Level Agreement which documents the performance expected and the remedies available in case of non compliance."

EXPLANATORY NOTES

This activity involves the employment of a firm to dispose of surplus materials and equipment. See also *Disposing of Obsolete Equipment*.

Information Security issues to be considered when implementing your policy include the following:

- Confidentiality of your information may be breached because the disposal firm does not specialise in handling confidential data securely.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.2.2 Security requirements from third party contracts
8.6.2 Disposal of media

Policy 030904
Using Photocopier for Personal Use

SUGGESTED POLICY STATEMENT

"The use of photocopiers or duplicators for personal use is discouraged. In exceptions, specific permission may be given by the employee's immediate supervisor or manager."

EXPLANATORY NOTES

If the organisation permits staff to use the photocopier for personal use then specific permission should be granted every time this is done.

Information Security issues to be considered when implementing your policy include the following:

- Permitting personal use provides greater opportunity to copy and remove sensitive material
- Allowing personal use may encourage the pilfering of paper and other resources.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.5 Prevention of misuse of information processing facilities

Policy 030905
Speaking to the Media

SUGGESTED POLICY STATEMENT

"Only authorised personnel may speak to the media (newspapers, television, radio, magazines etc.) about matters relating to the organisation."

EXPLANATORY NOTES

As most people are not trained to deal with the media, and they may not be aware of the significance of data passed to the media, many companies use designated spokespersons to handle media enquires. Small pieces of information, although insignificant in themselves, can be used to build a larger picture of more sensitive matters.

Information Security issues to be considered when implementing your policy include the following:

- Manipulation by journalists may result in unintentional disclosure of organisation information.
- Unauthorised disclosure of sensitive organisation data may result in confidential information becoming public knowledge.
- Information may be passed to the media unwittingly.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.3 Confidentiality agreements

Policy 030906
Speaking to Customers

SUGGESTED POLICY STATEMENT

"Information regarding the organisation's customers or other people dealing with the organisation is to be kept confidential at all times. The information should only released by authorised and trained persons."

EXPLANATORY NOTES

Dealing with customers is a highly skilled activity requiring interpersonal skills which strikes a balance between organisation needs and customer demands. Some organisations have a customer services department who are trained to handle customer queries or complaints. Employees should be alert to potential security risks when releasing information to customers.

Information Security issues to be considered when implementing your policy include the following:

- Confidential organisation data may be incorrectly released to unauthorised third parties.
- Information may be requested by unauthorised persons.
- Customers may request confidential data to be released.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.3 Confidentiality agreements
12.1.4 Data protection and privacy of personal information

Policy 030907
Need for Dual Control / Segregation of Duties

SUGGESTED POLICY STATEMENT

"The techniques of dual control and segregation of duties are to be employed to enhance the control over procedures wherever both the risk from, and consequential impact of, a related Information Security incident would likely result in financial or other material damage to the organisation."

EXPLANATORY NOTES

There is no way to completely prevent fraud in an organisation. However, *segregation of duties* is a primary internal control which prevents, or decreases the risk of errors, or irregularities, and identifies problems. This is achieved when an individual does not have control over all phases of a transaction. Likewise *dual control* is a simple means of ensuring that colleagues perform critical activities as a team.

Information Security issues to be considered when implementing your policy include the following:

- Information and resources may be accessed with the intent to defraud.
- In centralised computer environments, system administration and user activities should be separated otherwise sensitive data may be compromised.
- Fraudulent activities may be hidden, unless potential areas of fraud are identified and their duties segregated. The opportunity for fraud or errors is high where activities are not under dual control.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.1.4 Segregation of duties

Policy 030908
Using Clear Desk Policy

SUGGESTED POLICY STATEMENT

"This organisation expects all employees to operate a clear desk policy."

EXPLANATORY NOTES

With open plan offices now common you may accidentally expose confidential material. Information can be read from papers on your desk, especially when you away from your desk. A *Clear Desk Policy* is an effective safeguard.

Information Security issues to be considered when implementing your policy include the following:

- Material could be removed from your desk or work area and copied or stolen.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.3.1 Clear desk and clear screen policy

Policy 030909
Misaddressing Communications to Third Parties

SUGGESTED POLICY STATEMENT

"E-mail addresses and faxes are to be checked carefully prior to dispatch, especially where the information is considered to be confidential; and where the disclosure of the e-mail addresses or other contact information, to the recipients is a possibility."

EXPLANATORY NOTES

The risk of inadvertently passing information to unauthorised parties increases the higher the level of automation of your communication processes.

Information Security issues to be considered when implementing your policy include the following:

- You may send organisation data or information to unauthorised parties in error.
- Your e-mail distribution may disclose your entire customer and / or corporate mailing list details to each of the recipients.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.5 Security of electronic office systems

Policy 030910
Verifying Correctness of Information

SUGGESTED POLICY STATEMENT

"The organisation values the integrity and correctness of all its business and related information and requires management to develop and adopt the appropriate procedures in this regard."

EXPLANATORY NOTES

The integrity of information is fundamental to any organisation, and every effort must be made to implement the relevant safeguards, especially for data which falls under the *UK Data Protection Act* 1998 (or equivalent).

Information Security issues to be considered when implementing your policy include the following:

- Where controls and checks are not in place, the integrity of the organisation's data may not be reliable, which in turn can lead to the integrity of the entire organisation being compromised.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.2.4 Output data validation

Policy 030911
Travelling on Business

SUGGESTED POLICY STATEMENT

"Employees travelling on business are responsible for the security of information in their custody."

EXPLANATORY NOTES

Staff may be required to travel both locally and overseas as part of their work duties. Special care should be taken if using hotel facilities or commercial business centres.

Information Security issues to be considered when implementing your policy include the following:

- Documents stolen or misused whilst travelling.
- Where no personal security risk assessment is undertaken prior to travel, this can leave you unprepared for the real dangers which you may face at your destination.
- Inadequate classification of documents created whilst travelling can lead to inadvertent disclosure to unauthorised persons.
- Inadequate classification of documents created whilst travelling can lead to inadvertent disclosure to unauthorised persons.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.8.1 Mobile computing

Policy 030912
Checking Customer Credit Limits

SUGGESTED POLICY STATEMENT

"Credit may only be advanced to customers once credit limits have been properly approved, in accordance with the organisation's usual financial credit control procedures."

EXPLANATORY NOTES

Customer's credit limits to be checked before confirming any order placed on credit. When checking a customer's credit limit you are accessing sensitive information and therefore must observe the *UK Data Protection Act* or its local equivalent.

Information Security issues to be considered when implementing your policy include the following:

- Fraudulent credit applications result in loss or theft of goods.
- Unauthorised third parties may access customer details whilst credit checking a customer.
- An outsourced credit-checking agency will have access to confidential client details.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.4 Data protection and privacy of personal information

CHAPTER 04
PURCHASING AND MAINTAINING COMMERCIAL SOFTWARE

Sub-Chapter 01
Purchasing and Installing Software

Policy 040101
Specifying User Requirements for Software

SUGGESTED POLICY STATEMENT

"All requests for new applications systems or software enhancements must be presented to senior management with a Business Case with the business requirements presented in a User Requirements Specification document."

EXPLANATORY NOTES

Before deciding on the purchase of new software, it is essential to specify the business and technical requirements that are to be met. This is usually accomplished by means of a *User Requirements Specification* (URS).

Information Security issues to be considered when implementing your policy include the following:

- A failure to specify requirements precisely can result in an inappropriate choice of a system that is unable to meet business needs and expectations.
- A business which does not explore the issues from both technical and business perspectives can have such weaknesses exposed during the project, resulting in additional costs and loss of time.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.4 Authorisation process for information processing facilities

Policy 040102
Selecting Business Software Packages

SUGGESTED POLICY STATEMENT

"The organisation should generally avoid the selection of business critical software which, in the opinion of management, has not been adequately proven by the early adopters of the system. The selection process for all new business software must additionally incorporate the criteria upon which the selection will be made. Such criteria must receive the approval of senior management."

EXPLANATORY NOTES

Except where there is a clear *Business Case* to justify the expenditure for bespoke software, the majority of your software is likely to be *packaged*. Selecting the right package is critical, because it is expensive to correct mistakes later, and will have consequences for years to come.

N.B. This policy concerns software systems which directly support your business processes, e.g. Accounting and General Ledger, Sales, Order Processing, Inventory Control, and so forth, rather than *selecting office software packages* for word processors, e-mail, etc.

Information Security issues to be considered when implementing your policy include the following:

- Selecting a package which fails to meet your business needs can not only result in direct financial loss, but inevitably wastes time and resources.
- Whilst the software may meet your requirements functionally, lack of available support will increase the risk to your systems processing, and hence the businesses which are reliant upon it.
- Many mature systems have been written for proprietary operating systems which require daily support duties that rely on skills that are possibly less common. The possible inadvertent neglect of such duties may result in failures which endanger your business operations.
- The specification of your current equipment may be too low (or only marginally adequate), resulting in strain and overload which could corrupt information if the system were to crash.
- Business software is usually expected to work with other attached *peripherals*, e.g. fax, scanner, modem, printers, etc. However, and especially with older equipment, the *drivers* may be obsolete and only operate with certain software etc.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.4 Authorisation process for information processing facilities

Policy 040103
Selecting Office Software Packages

SUGGESTED POLICY STATEMENT

"All office software packages must be compatible with the organisation's preferred and approved computer operating system and platform."

EXPLANATORY NOTES

Office software forms a critical link between the primary business systems in your day to day work. The initial choice of the office package has far reaching consequences; both for the selection of additional software in the future and for the ease with which documents and information can be shared throughout the organisation.

N.B. This policy is aimed primarily at those using the Microsoft Windows® operating system. However, the issues and actions are applicable to all *platforms*.

Information Security issues to be considered when implementing your policy include the following:

- Office software, pre-installed by your hardware supplier, may not meet your organisation's needs. You can then become 'locked into' unsuitable systems and effectively prevented from the correct choice of office software.
- Lack of set organisation standards can allow the user's personal preferences to determine the choice of office software. This can cause delays and frustration, with information being inaccessible to anyone not using the same office software, or using a different version.
- Where support for an old office system is poor or where the product has been discontinued for some time, you are exposed in case of system failure or other problem. You could lose information, simply because it can no longer be read.

  N.B. The above is **not** an example of the adage "If it ain't broke, don't fix it"! This issue is unlikely to go away. If anything, it will worsen over time and possible force a change when it is least convenient.
- The use of separate office products across the organisation introduces the real (and likely) risk of incompatible data formats.
- The specification of your current equipment may be too low or only marginally adequate, resulting in strain and overload which could corrupt information if the system were to *crash*.
- Office software is usually expected to work with other attached *peripherals*, e.g. fax, scanner, modem, printers, etc. However, and especially with older equipment, the *drivers* may be obsolete and only operate with certain software etc.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.4 Authorisation process for information processing facilities

Policy 040104
Using Licensed Software

SUGGESTED POLICY STATEMENT

"To comply with legislation and to ensure ongoing vendor support, the terms and conditions of all End User Licence Agreements are to be strictly adhered to."

EXPLANATORY NOTES

You must be licensed to use software and also adhere to the terms of the *End User License Agreement* (EULA). This is necessary to comply with legal requirements and to retain your eligibility for ongoing vendor support.

Information Security issues to be considered when implementing your policy include the following:

- Using unlicensed software that is not being evaluated under the terms of the licence, is a criminal offence in many countries. Both the individual concerned and the directors (or equivalent) of the organisation may be held accountable.
- Where licence restrictions come to light following a period of use, there may be additional and unexpected costs.
- Allowing software to expire or be unlicensed can result in the vendor's refusal to provide support and / or upgrades at a reasonable price. For those areas which rely upon the software in question, this places both the business processes and the resultant information at risk.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.2.2 Software copyright

Policy 040105
Implementing New / Upgraded Software

SUGGESTED POLICY STATEMENT

"The implementation of new or upgraded software must be carefully planned and managed, ensuring that the increased Information Security risks associated with such projects are mitigated using a combination of procedural and technical control techniques."

EXPLANATORY NOTES

All software (from the operating system to applications) needs to be updated periodically. Whether this is a simple upgrade or a complete re-write of your main system, it involves a series of steps, whose length depends on the size and complexity of the system.

Information Security issues to be considered when implementing your policy include the following:

- Where a new system is inadequately tested, it can result in substantial damage to the business processes that rely on it, and to the data files it reads and updates.
- Considering security requirements of a system as an afterthought may expose the organisation to loss or fraud.
- Inadequate training for both technical and user staff, can result in costly errors in information content and in business processing. This may compromise other systems that rely on them.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.1 Security requirements of systems

Sub-Chapter 02
Software Maintenance & Upgrade

Policy 040201	**Applying 'Patches' to Software**
Policy 040202	**Upgrading Software**
Policy 040203	**Responding to Vendor Recommended Upgrades to Software**
Policy 040204	**Interfacing Applications Software / Systems**
Policy 040205	**Supporting Application Software**
Policy 040206	**Operating System Software Upgrades**
Policy 040207	**Support for Operating Systems**
Policy 040208	**Recording and Reporting Software Faults**

Policy 040201
Applying 'Patches' to Software

SUGGESTED POLICY STATEMENT

"Patches to resolve software bugs may only be applied where verified as necessary and with management authorisation. They must be from a reputable source and are to be thoroughly tested before use."

EXPLANATORY NOTES

Patches are software bug 'fixes', that is, they resolve problems reported by users. Usually available for downloading on the vendor's Web site, their use requires consideration of the relevant security issues.

Information Security issues to be considered when implementing your policy include the following:

- If a patch is applied incorrectly or without adequate testing, your system and its associated information can be placed at risk, possibly corrupting your live data files.
- If patches are not reviewed and tested, important security fixes may leave your systems exposed. This is especially true of 'office' software.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.5.1 Change control procedures

Policy 040202
Upgrading Software

SUGGESTED POLICY STATEMENT

"Upgrades to software must be properly tested by qualified personnel before they are used in a live environment."

EXPLANATORY NOTES

The status of software is rarely static. Software companies are either releasing bug fixes (*patches*), or introducing new versions with enhanced functionality. However, substantial Information Security issues are raised by this seemingly straight forward process.

Information Security issues to be considered when implementing your policy include the following:

- The new version may simply fail to perform as expected and / or may have key features removed, enhanced or otherwise modified - potentially disrupting your business operations.
- Users of an older version of the software can be prevented from reading files created using a later release of the software.
- New software versions released following the merger of software companies may contain unanticipated (new) code and / or bugs.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.2.2 System acceptance
10.5.1 Change control procedures

Policy 040203
Responding to Vendor Recommended Upgrades to Software

SUGGESTED POLICY STATEMENT

"The decision whether to upgrade software is only to be taken after consideration of the associated risks of the upgrade and weighing these against the anticipated benefits and necessity for such change."

EXPLANATORY NOTES

Although software may be operating satisfactorily, vendors will promote the latest releases to make additional sales and to *migrate* all customers to a common version. This reduces their support costs and improves service levels. However, upgrades usually entail risks.

Information Security issues to be considered when implementing your policy include the following:

- Where *legacy* software is running on an older operating system, the supplier may announce that the next release will no longer be available for that *platform* but for (say) Windows® 2000 or NT. This sounds straightforward, but it is important to consider the implications in order to avoid making rash decisions. There can be more than a single project to consider:-
- A hardware migration / upgrade.
- An operating system migration / upgrade.
- A new version of the applications software to review, test and implement.
- A possible migration of data files to the new hardware and any interfaces which integrate to other systems.
- In order to enhance functionality, the data file formats and processing routines may have been modified. This might lead to problems in using your data and established information handling routines.
- Reduced support for your (older) version of the system can mean delayed response time or even a failure to resolve problems.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.2.2 System acceptance
10.5.1 Change control procedures

Policy 040204
Interfacing Applications Software / Systems

SUGGESTED POLICY STATEMENT

"Developing Interfacing software systems is a highly technical task and should only be undertaken in a planned and controlled manner by properly qualified personnel."

EXPLANATORY NOTES

Many software packages can exchange data and link with a variety of popular systems. Such *interfaces* often need to be specially developed for bespoke or *legacy* systems. Interfacing can be a complex process requiring data first to be exported from one system, then *massaged*, and finally imported into the target system. This process puts your data at great risk.

Information Security issues to be considered when implementing your policy include the following:

- The purchase of a new system may have been agreed on the basis of the apparent ease of interfacing to your current system(s). Interfacing problems can result in substantial delays and even cause entire projects to fail, especially where complex data *massaging* is required.
- Where an interface program is required to reformat the data to meet the needs of the target system, such data *massaging* poses a risk of data modification (possibly maliciously) and, thereby, inaccurate processing.
- Temporary files, created by interface program processing, and saved in a temporary location, may contain sensitive data which unauthorised persons might access, thus compromising the *confidentiality* of your information.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.1.1 Security requirements analysis and specification
10.5.2 Technical review of operating system changes

Policy 040205
Supporting Application Software

SUGGESTED POLICY STATEMENT

"All application software must be provided with the appropriate level of technical support to ensure that the organisation's business is not compromised by ensuring that any software problems are handled efficiently with their resolution available in an acceptable time."

EXPLANATORY NOTES

The adequacy of your routine applications support ('Help Desk') can greatly influence the frequency and severity of problems you experience. Where such support is not readily available, technical staff and users may try to fix problems themselves following various (possibly random) ideas, and in so doing, compromise security.

Information Security issues to be considered when implementing your policy include the following:

- Where a system has a poor or inadequate level of support, this may compromise Information Security, as both users and local technical staff try to fix / patch up the problem.
- In their frustration, users may call upon the office 'power user' to resolve problems, who in turn may implement a 'quick and dirty' solution. Security can also be compromised if the 'power user' is offered the users' passwords as they attempt to solve the problem.
- Furthermore such 'ad hoc' solutions are rarely documented and followed up with the vendor which can prolong the resolution of the problem.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.2.2 Security requirements in third party contracts
10.5 Security in development and support processes

Policy 040206
Operating System Software Upgrades

SUGGESTED POLICY STATEMENT

"Necessary upgrades to the Operating System of any of the organisation's computer systems must have the associated risks identified and be carefully planned, incorporating tested fall-back procedures. All such upgrades being undertaken as a formal project."

EXPLANATORY NOTES

Like any other system, the *operating system* (OS) of a computer uses software, which, from time to time, requires *patches* and upgrades. However, unlike individual application software upgrades, problems with OS upgrades can impact on all applications running on the computer, and also on users logged on directly, or via the network.

Information Security issues to be considered when implementing your policy include the following:

- Where an upgraded OS fails to perform as expected, it can jeopardise your entire system and possibly also the network. The impact can be disastrous.
- If security aspects of the OS upgrade are addressed inadequately or overlooked, this significantly increases risk, especially from those with technical know-how who may exploit the weaknesses.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.5.2 Technical review of operating system changes

Policy 040207
Support for Operating Systems

SUGGESTED POLICY STATEMENT

"Operating Systems must be regularly monitored and all required 'housekeeping' routines adhered to."

EXPLANATORY NOTES

The operating system of desktop systems within your organisation will generally run without substantial interference. However, for servers, mini-computers and mainframes, especially those running mature *Operating Systems* (OS), day to day *housekeeping* is usually required.

Information Security issues to be considered when implementing your policy include the following:

- Where an upgraded operating system fails to perform as expected, this can result in a loss of *stability* or even the total failure of some systems.
- Where housekeeping and routine support are informal or incident led, weaknesses in the security safeguards can go undetected and offer the potential for fraud or malicious damage.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.5.2 Technical review of operating system changes

Policy 040208
Recording and Reporting Software Faults

SUGGESTED POLICY STATEMENT

"Software faults are to be formally recorded and reported to those responsible for software support / maintenance."

EXPLANATORY NOTES

A software fault prevents the proper and reliable use of an application or feature, although reputable software and correct procedures have been used. A software incident becomes a 'fault' when the investigator has disproved other factors, such as user error. An 'incident' is an unexpected event or result which in itself may be minor but may be symptomatic of a larger problem or may signal an actual or potential security breach. All incidents must be taken seriously.

Information Security issues to be considered when implementing your policy include the following:

- Errors are compounded due to delays in fault or incident reporting.
- Insufficient data may lead to incorrect diagnosis of the fault or may hide a possible security breach.
- Where there are no procedures to monitor reported faults or to undertake trend analysis, the underlying source of the problem may go undetected.
- No procedures in place to handle software fault reporting.
- Lack of any proactive preventative maintenance.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.4.3 Fault logging

Sub-Chapter 03
Other Software Issues

Policy 040301 Disposing of Software

Policy 040301
Disposing of Software

SUGGESTED POLICY STATEMENT

"The disposal of software should only take place when it is formerly agreed that the system is no longer required and that its associated data files which may be archived will not require restoration at a future point in time."

EXPLANATORY NOTES

Software is often licensed indefinitely. However, a change of organisation circumstances may result in a decision to stop using a certain system or to move to another. The removal and disposal of the software needs to be considered.

Information Security issues to be considered when implementing your policy include the following:

- Disposing of software without adequate consideration could cause great difficulties, especially where you need to restore the application's data files from backup.
- If previous version(s) of software are disposed of prematurely, it may be impossible to revert to the old software when problems are encountered with the latest release.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.2 Disposal of media

CHAPTER 05
DEVELOPING AND MAINTAINING IN-HOUSE SOFTWARE

Sub-Chapter 01
Controlling Software Code

Policy 050101	**Managing Operational Program Libraries**
Policy 050102	**Managing Program Source Libraries**
Policy 050103	**Controlling Software Code during Software Development**
Policy 050104	**Controlling Program Listings**
Policy 050105	**Controlling Program Source Libraries**
Policy 050106	**Controlling Old Versions of Programs**

Policy 050101
Managing Operational Program Libraries

SUGGESTED POLICY STATEMENT

"Only designated staff may access operational program libraries. Amendments may only be made using a combination of technical access controls and robust procedures operated under dual control."

EXPLANATORY NOTES

Managing the directories within your computer system(s) in which operational (live) software is stored.

Information Security issues to be considered when implementing your policy include the following:

- If your operational program libraries are poorly protected, your software and configuration files could be modified without authorisation, resulting in disruption to your system and / or other incidents.
- Unauthorised use of *production* software can cause disruption to your systems or fraud against your organisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.4.1(a) Control of operational software
10.5.1 Change control procedures

Policy 050102
Managing Program Source Libraries

SUGGESTED POLICY STATEMENT

"Only designated staff may access program source libraries. Amendments may only be made using a combination of technical access controls and robust procedures operated under dual control."

EXPLANATORY NOTES

Managing the directory areas within your system where the source code and object code of your live and development systems are held. Live and development libraries must always be kept separate.

Information Security issues to be considered when implementing your policy include the following:

- Lack of the source code can make it difficult or impossible to maintain your systems.
- Unauthorised amendment of source code can result in system failures and / or malicious damage.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.4.3 Access control to program source library
10.5.1 Change control procedures

Policy 050103
Controlling Software Code during Software Development

SUGGESTED POLICY STATEMENT

"Formal change control procedures must be utilised for all changes to systems. All changes to programs must be properly authorised and tested before moving to the live environment."

EXPLANATORY NOTES

Although many systems are based upon standard *package* software, many organisations nevertheless continue to develop software, either as maintenance of a legacy system, or because their needs are unique and competitive advantage is gained by their specialised capability. As a result, even relatively small organisations can find themselves managing a team of 'development' staff. This policy identifies some of the key Information Security issues related to such risks.

Information Security issues to be considered when implementing your policy include the following:

- Insufficient testing of new software can often result in errors which disrupt your operational systems.
- Where software coding standards have not been agreed, on going maintenance can become onerous because the structure of the code is inconsistent.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.5.1 Change control procedures
10.5.3 Restrictions on changes to software packages

Policy 050104
Controlling Program Listings

SUGGESTED POLICY STATEMENT

"Program listings must be controlled and kept fully up to date at all times."

EXPLANATORY NOTES

Controlling the printouts or reports, electronic or hard copy, of the application source code which makes up the programs run on your system.

Information Security issues to be considered when implementing your policy include the following:

- Loss or unavailability of a listing can result in delays in identifying the source of a system problem, the result of which could be severe.
- Having a program listing available can used by anyone with ill intent or seeking to defraud, as it gives them the precise logic and routines for the system in question.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.4 Security of system documentation
10.4.3(f) Access control to program source library

Policy 050105
Controlling Program Source Libraries

SUGGESTED POLICY STATEMENT

"Formal change control procedures with comprehensive audit trails are to be used to control Program Source Libraries."

EXPLANATORY NOTES

Monitoring and investigating changes made to your program source libraries.

Information Security issues to be considered when implementing your policy include the following:

- Any unauthorised changes made to the program source libraries can open the door to potential error or fraud.
- If audit trail reports and event logs are not regularly reviewed, incidents can remain undetected.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.4.3 Access control to program source library
10.5.1 Change control procedures

Policy 050106
Controlling Old Versions of Programs

SUGGESTED POLICY STATEMENT

"Formal change control procedures with comprehensive audit trails are to be used to control versions of old programs."

EXPLANATORY NOTES

Controlling the way in which you handle the application code of programs within your system which has been superseded or discontinued.

Information Security issues to be considered when implementing your policy include the following:

- If the program library has been removed or updated, you may not be able to access or revert to the older version of the application if need be. This could cause severe problems where there are found to be major *bugs* in the newer version.
- Beware of old versions of programs being confused with the latest version, resulting either in the loss of recent enhancements or a failure of other systems, which depend on recent features.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.4.1 Control of operational software
10.5.1 Change control procedures

Sub-Chapter 02
Software Development

Policy 050201	**Software Development**
Policy 050202	**Making Emergency Amendments to Software**
Policy 050203	**Establishing Ownership for System Enhancements**
Policy 050204	**Justifying New System Development**
Policy 050205	**Managing Change Control Procedures**
Policy 050206	**Separating Systems Development and Operations**

Policy 050201
Software Development

SUGGESTED POLICY STATEMENT

"Software developed for or by the organisation must always follow a formalised development process which itself is managed under the project in question. The integrity of the organisation's operational software code must be safeguarded using a combination of technical access controls and restricted privilege allocation and robust procedures."

EXPLANATORY NOTES

Unless carefully managed, that which begins as a minor modification to a *script* can migrate into an informal systems development effort, but with none of the necessary controls and safeguards to protect the live operations of the organisation.

Information Security issues to be considered when implementing your policy include the following:

- Where programmers work as independent units, bad or malicious code could be copied into the source code with malicious or fraudulent intent; and no one would know - until it was too late.
- Software under development can become confused with operational software and potentially disrupt live operations.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.1.5 Separation of development and operational facilities
10.1.1 Security requirements analysis and specification
10.5.1 Change control procedures

Policy 050202
Making Emergency Amendments to Software

SUGGESTED POLICY STATEMENT

"Emergency amendments to software are to be discouraged, except in circumstances previously designated by management as 'critical'. Any such amendments must strictly follow agreed change control procedures."

EXPLANATORY NOTES

The emergency measures that you should adopt if it becomes necessary to amend the live software environment **immediately**.

Information Security issues to be considered when implementing your policy include the following:

- Emergency conditions can lead to a collapse of agreed procedures with the resultant opportunity for error or malicious activity.
- Rushed changes can result in additional errors / bugs which compound the problem.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.5.1 Change control procedures

Policy 050203
Establishing Ownership for System Enhancements

SUGGESTED POLICY STATEMENT

"All proposed system enhancements must be business driven and supported by an agreed Business Case. Ownership (and responsibility) for any such enhancements will intimately rest with the business owner of the system."

EXPLANATORY NOTES

Ensuring that users recognise and accept their responsibilities for enhancements, which should always be driven by the needs of the business rather than being 'IT lead'.

Information Security issues to be considered when implementing your policy include the following:

- System enhancements can be ill-defined, poorly analysed or inadequately tested and, as a consequence, endanger your business operations.
- Where a business case is not developed, or developed poorly, the anticipated benefits from the enhancements may be ill-conceived and hence never materialise.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.3 Allocation of information security responsibilities

Policy 050204
Justifying New System Development

SUGGESTED POLICY STATEMENT

"The development of bespoke software is only to be considered, if warranted by a strong Business Case and supported both by management and adequate resources over the projected life time of the resultant project."

EXPLANATORY NOTES

Developing a system 'from scratch', as opposed to enhancing a present system, represents a major decision, and quite possibly a significant risk. The *Business Case* for a *bespoke* development must be very strong indeed to reject the selection of a suitable *packaged* solution.

Information Security issues to be considered when implementing your policy include the following:

- The risk of failure of a bespoke development can be extremely high and could pose a substantial risk to the business.
- Senior Management support and financial backing can fluctuate - especially in a project lasting more than 12 months. Reduced commitment and support can result in project failure and hence loss.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.4 Authorisation process for information processing facilities
10.1.1 Security requirements analysis and specification

Policy 050205
Managing Change Control Procedures

SUGGESTED POLICY STATEMENT

"Formal change control procedures must be utilised for all amendments to systems. All changes to programs must be properly authorised and tested in a test environment before moving to the live environment."

EXPLANATORY NOTES

Change Control ensures that all changes are analysed and authorised. The Management of the process is used to enforce the requirement.

Information Security issues to be considered when implementing your policy include the following:

- Any amendment to your systems environment can result in Information Security weaknesses which could be exploited to the detriment of business operations.
- Seemingly harmless changes to your business process (e.g. Sales Order Processing) can introduce weaknesses which could damage both this and any associated processes.
- If formal change control procedures are not implemented, it can be very difficult to manage changes on a prioritised basis.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.5.1 Change control procedures

Policy 050206
Separating Systems Development and Operations

SUGGESTED POLICY STATEMENT

"Management must ensure that proper segregation of duties applies to all areas dealing with systems development, systems operations, or systems administration."

EXPLANATORY NOTES

Whilst only the larger organisations are likely to have separate *Systems Operations* and *Systems Development* sections or departments, it is nevertheless vital to separate these functions. Such a *segregation of duties* lies at the heart of most Information Security safeguards.

Information Security issues to be considered when implementing your policy include the following:

- Live data or software could be amended or modified by IT staff, either accidentally or for vindictive or fraudulent reasons.
- The running of test code will often contain 'de-bug' code and possibly other error trapping routines which impose a substantially high overhead on the host system.
- Development staff will often operate with powerful privileges which, in an operational environment, would be high risk and hence unacceptable.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.1.4 Segregation of Duties
8.1.5 Separation of development and operational facilities

Sub-Chapter 03
Testing & Training

Policy 050301	**Controlling Test Environments**
Policy 050302	**Using Live Data for Testing**
Policy 050303	**Testing Software before Transferring to a Live Environment**
Policy 050304	**Capacity Planning and Testing of New Systems**
Policy 050305	**Parallel Running**
Policy 050306	**Training in New Systems**

Policy 050301
Controlling Test Environments

SUGGESTED POLICY STATEMENT

"Formal change control procedures must be employed for all amendments to systems. All changes to programs must be properly authorised and tested in a test environment before moving to the live environment."

EXPLANATORY NOTES

The control process to keep system testing separate from live, operational work.

Information Security issues to be considered when implementing your policy include the following:

- The inappropriate introduction of modified software can have potentially disastrous results and bring the organisation to a standstill.
- IT staff who run day to day operations and also test new software, (possibly swapping from one to the other on the same screen),risk making unintentional errors by inadvertently issuing system commands to the wrong system.
- Testing a system at the same time as it is being used for development work can yield flawed test results and give an inaccurate picture of its readiness for live operations.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.2.2 System acceptance
10.5.1 Change control procedures

Policy 050302
Using Live Data for Testing

SUGGESTED POLICY STATEMENT

"The use of live data for testing new system or system changes may only be permitted where adequate controls for the security of the data are in place."

EXPLANATORY NOTES

Ideally, all testing would utilise only realistic test data, expressly created for the purpose. However, in practice that may not be feasible, and it may be necessary to use a copy of current data files e.g. the client database. It is imperative that any such 'temporary test data' be treated as live at all times. This is particularly important because test staff tend to have more system privileges compared to a *live (production)* environment, and the organisation's usual Information Security procedures are unlikely to be followed.

Information Security issues to be considered when implementing your policy include the following:

- Using live data for testing can severely compromise its confidentiality, possibly even leading to legal action.
- The acquisition of data for testing may breach the Information Security safeguards of your live system which could result in fraud, malicious damage or even legal action if confidentiality is lost.
- Data used for testing can become merged with live data, leading to confusion and potential disruption to your business operations.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

10.4.2 Protection of system test data

Policy 050303
Testing Software before Transferring to a Live Environment

SUGGESTED POLICY STATEMENT

"Formal change control procedures must be utilised for all amendments to systems. All changes to programs must be properly authorised and tested in a test environment before moving to the live environment."

EXPLANATORY NOTES

Employing procedures to ensure that your software programs are fully tested and documented before they are made available for live or operational use.

Information Security issues to be considered when implementing your policy include the following:

- Inadequately tested software can have potentially disastrous results, bringing the organisation to a standstill; for example by crashing suddenly and corrupting the data files.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.2.2 System acceptance
10.5.1 Change control procedures

Policy 050304
Capacity Planning and Testing of New Systems

SUGGESTED POLICY STATEMENT

"New systems must be tested for capacity, peak loading and stress testing. They must demonstrate a level of performance and resilience which meets or exceeds the technical and business needs and requirements of the organisation."

EXPLANATORY NOTES

The *System Testing* process should verify that new or amended systems are able to handle the expected transaction volumes, delivering both acceptable performance and resilience.

Information Security issues to be considered when implementing your policy include the following:

- *System Testing* based upon data which is not representative of actual volumes and peak loading will give potentially misleading results and may, if migrated to live operations, jeopardise the continued running of your systems.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.2.1 Capacity planning
8.2.2 System acceptance

Policy 050305
Parallel Running

SUGGESTED POLICY STATEMENT

"Normal System Testing procedures will incorporate a period of parallel running prior to the new or amended system being acceptable for use in the live environment. The results of parallel running should not reveal problems or difficulties which were not previously passed during User Acceptance Testing."

EXPLANATORY NOTES

The process of running a new or amended system simultaneously with the old system to confirm that it functions correctly before going live.

Information Security issues to be considered when implementing your policy include the following:

- Despite *System Testing* and *User Acceptance Testing* the performance of your new system can differ unexpectedly from the old system and threaten to delay day-to-day processing.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.2.2 System acceptance
10.5.1 Change control procedures

Policy 050306
Training in New Systems

SUGGESTED POLICY STATEMENT

"Training is to be provided to users and technical staff in the functionality and operations of all new systems."

EXPLANATORY NOTES

Ensuring that all users, whether business or technical, are adequately trained in the use of all new and enhanced systems.

Information Security issues to be considered when implementing your policy include the following:

- Where training of both business and technical staff is not viewed as a priority, apparently small problems can escalate due to inadequate knowledge.
- Of particular importance when training staff in new systems is the understanding and application of the information security processes inherent in those systems.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.2.1 Information security education and training

Sub-Chapter 04
Documentation

Policy 050401 Documenting New and Enhanced Systems

Policy 050401
Documenting New and Enhanced Systems

SUGGESTED POLICY STATEMENT

"All new and enhanced systems must be fully supported at all times by comprehensive and up to date documentation. New systems or upgraded systems should not be introduced to the live environment unless supporting documentation is available."

EXPLANATORY NOTES

Ensuring that new and enhanced systems are adequately documented. All too often, due to budget and other resource limitations, documentation can be limited or even totally ignored. The Information Security threats become substantial - especially where changes and amendments are required, possibly at short notice for regulatory or other reasons.

Information Security issues to be considered when implementing your policy include the following:

- When a sudden problem occurs on the system, a lack of adequate documentation can greatly increase the risk of serious mishap. 'Fixes' may be based upon staff experience and not supported by the original developer's documentation.
- Missing, out-dated or incomplete documentation can severely compromise the organisation's ability to maintain its software and systems.
- Without documentation it still remains possible to perform a *peer review* of the source code, but its effectiveness is reduced and can allow errors and omissions to slip through, into *System Testing* and perhaps beyond, into *User Acceptance Testing*.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.1.1 Inventory of assets
8.6.4 Security of system documentation

Sub-Chapter 05
Other Software Development

Policy 050501 Acquiring Vendor Developed Software

Policy 050501
Acquiring Vendor Developed Software

SUGGESTED POLICY STATEMENT

"Vendor developed software must meet the User Requirements Specification and offer appropriate product support."

EXPLANATORY NOTES

Acquiring software that is provided by outside suppliers, either as a package or as a bespoke development to meet the specific needs of your organisation.

Information Security issues to be considered when implementing your policy include the following:

- The expected features of the software (the 'functionality'), if missing or inadequate, can make it difficult or impossible to meet the targets for the system in question.
- Inadequate support by the vendor can make it difficult, or impossible, to operate the system as expected thus compromising your business operations.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.2.2(n) Security requirements in third party contracts

CHAPTER 06
COMBATING CYBER CRIME

Sub-Chapter 01 Combating Cyber Crime

Sub-Chapter 01
Combating Cyber Crime

Policy 060101
Defending Against Premeditated Cyber Crime Attacks

SUGGESTED POLICY STATEMENT

"Security on the network is to be maintained at the highest level. Those responsible for the network and external communications are to receive proper training in risk assessment and how to build secure systems which minimise the threats from cyber crime."

EXPLANATORY NOTES

There is a very high risk of external security breaches where network security is inadequate.

Information Security issues to be considered when implementing your policy include the following:

- Criminals may target your organisation's information systems, resulting in serious financial loss and damage to your business operations and reputation.
- Cyber crime is an ever increasing area of concern, and suitable training is to be given to those persons responsible for network security to minimise such risks.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.4 Network access control

Policy 060102
Minimising the Impact of Cyber Attacks

SUGGESTED POLICY STATEMENT

"Plans are to be prepared, maintained and regularly tested to ensure that damage done by possible external cyber crime attacks can be minimised and that restoration takes place as quickly as possible."

EXPLANATORY NOTES

Even the most Information Security conscious organisations can be attacked; this may be to 'prove a point' or for other malicious reasons.

Information Security issues to be considered when implementing your policy include the following:

- Successful cyber attacks are likely to result in either a loss or corruption / theft of data, and possibly the disabling of services.
- Cyber crime can have a severe and immediate impact on your systems. Without proper planning for such events your business may not be able to recover within an acceptable timeframe.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

11.1.2 Business continuity and impact analysis

Policy 060103
Collecting Evidence for Cyber Crime Prosecution

SUGGESTED POLICY STATEMENT

"Perpetrators of cyber crime will be prosecuted by the organisation to the full extent of the law. Suitable procedures are to be developed to ensure the appropriate collection and protection of evidence."

EXPLANATORY NOTES

In order to prosecute Cyber Crime successfully you need proof. This can be difficult to provide, unless your organisation's information systems have adequate controls and audit capabilities.

Information Security issues to be considered when implementing your policy include the following:

- Lack of a clear trail of evidence when investigating cyber crime may prevent you taking legal action against suspects, and allow the perpetrator(s) to initiate further attacks.
- The security of your information systems may be compromised by the investigations of law enforcement agencies, e.g. In some countries, legislation grants law enforcement agents access to cryptographic keys, or to the unencrypted contents of data previously encrypted.
- The ***Regulation of Investigatory Powers Act***, enacted in 2000, provides such powers to UK law enforcement agencies.
- The Council of Europe - **Draft Convention on Cyber Crime**, released in late 2000, proposes even greater investigatory powers.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.7 Collection of evidence

Policy 060104
Defending Against Premeditated Internal Attacks

SUGGESTED POLICY STATEMENT

"In order to reduce the incidence and possibility of internal attacks, access control standards and data classification standards are to be periodically reviewed whilst maintained at all times."

EXPLANATORY NOTES

Identifying staff actions as criminal is beset with difficulties.
Access to confidential data may be legitimised in employees' job descriptions. The act of copying sensitive data may not necessarily leave a 'footprint' on the system, and such copies can then be exported from your organisation by e-mail or by removable media without leaving a trace. The effects of outright malicious data destruction are obvious, but the computer entry process of so doing may have seemed routine.

Information Security issues to be considered when implementing your policy include the following:

- A member of staff may target confidential information, or deface the organisation's web site, which could result in both financial loss and embarrassment (and possibly legal proceedings).
- The principle means of building defences against internal malicious attacks includes strong access control, high levels of staff awareness and vigilance.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.1.1 Access control policy
9.6.1 Information access restriction
9.7.2 Monitoring system use

Policy 060105
Defending Against Opportunistic Cyber Crime Attacks

SUGGESTED POLICY STATEMENT

"It is a priority to minimise the opportunities for cyber crime attacks on the organisation's systems and information through a combination of technical access controls and robust procedures."

EXPLANATORY NOTES

Opportunistic criminal attacks usually arise from chance discovery of a loophole in the system, which permits access to unauthorised information.

Information Security issues to be considered when implementing your policy include the following:

- Your Web site or data processing systems may be penetrated, allowing both the disclosure of sensitive information and also possibly the modification or corruption of the data. All such events can lead to public embarrassment and financial loss.
- Without an effective risk management process, it may be impossible to identify weak security defences before they are breached.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.4 Network access control

Policy 060106
Safeguarding Against Malicious Denial of Service Attack

SUGGESTED POLICY STATEMENT

"Contingency plans for a denial of service attack are to be maintained and periodically tested to ensure adequacy."

EXPLANATORY NOTES

Denial of Service (DoS) attacks have gained notoriety as being an effective way to disable Web based services. See ***Denial of Service*** for an explanation of the techniques used and their consequences.

Information Security issues to be considered when implementing your policy include the following:

- Your Web server(s) may be subjected to a DoS attack, which could result in damage to your organisation's reputation and also financial loss.
- If the responsible officials nominated to handle potential DoS attacks are not properly trained, then normal service is unlikely to be restored within an acceptable period.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.1.3(a) Incident management procedures
9.4 Network access control

Policy 060107
Defending Against Hackers, Stealth- and Techno-Vandalism

SUGGESTED POLICY STATEMENT

"Risks to the organisation's systems and information are to be minimised by fostering staff awareness, encouraging staff vigilance, and deploying appropriate protective systems and devices."

EXPLANATORY NOTES

Unlike other forms of Cyber Crime, these attacks take a 'scatter gun' approach, in that they do not target a specific organisation. If you happen to be 'in the firing line', and your Information Security safeguards are poor, you are likely to be hit. Such attacks may take the form of *time-*, *stealth*- and *logic*- bombs, e-mail attachments with *malicious code* and *Trojan Horses*.

Information Security issues to be considered when implementing your policy include the following:

- Malicious code which can replicate itself, may be downloaded unwittingly and executed. Having damaged your system, it can continue to wreak havoc with the systems of **other organisations and individuals**.
- E-mail may contain *malicious code*, which may replicate itself to all addresses within your organisation's e-mail system, and then corrupt the system of each recipient, **without the attachment even having been opened.**

N.B. Such replication is not restricted to your organisation's network, it can spread to those of your clients and suppliers; possibly destroying your reputation and business.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.1 Accountability for assets
6.1.1 Including security in job responsibilities
6.2.1 Information security education and training
9.4 Network access control

Policy 060108
Handling Hoax Virus Warnings

SUGGESTED POLICY STATEMENT

"Procedures to deal with hoax virus warnings are to be implemented and maintained."

EXPLANATORY NOTES

Threats from viruses are well known throughout the IT community. Hoax threats - the spreading of rumours of fictitious viruses or other malicious code - can waste time, as staff attempt to locate a virus which does not exist.
Vigilance and good virus intelligence warnings are the key to minimising the impact of hoaxes.

Information Security issues to be considered when implementing your policy include the following:

- If no one in your organisation is responsible for managing virus alerts, a genuine threat may be misconstrued as a hoax. This could jeopardise Information Security, since new virus variants may have no effective vaccine.
- Hoax threats can deflect attention from the threat from genuine viruses and other *malicious code*, increasing your susceptibility to 'infection'.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.3 Allocation of information security responsibilities
8.3.1 Controls against malicious software

Policy 060109
Defending Against Virus Attacks

SUGGESTED POLICY STATEMENT

"Without exception, Anti Virus software is to be deployed across all PCs with regular virus definition updates and scanning across both servers, PCs and laptop computers."

EXPLANATORY NOTES

Virus infection can be minimised by deploying proven anti-virus software and regularly updating the associated vaccine files. Many anti-virus companies supply such updates from their Web sites.

Information Security issues to be considered when implementing your policy include the following:

- Where no agreed response plan is in place, the reactions of users, IT and management are likely to be ad hoc and inadequate, thus possibly turning a containable incident into a significant problem.
- Lack of an agreed standard or inconsistent deployment of anti-virus software can seriously increase the risk of infection, spread and damage.
- Failing to update the virus definition files on a regular basis increases the risk of infection from a variant for which you do not have the necessary vaccine. This can cause great damage
- A failure to run regular virus scans across all data files on your server(s) reduces the ability to detect and cure a virus **before** its 'footprint' is identified by a user trying to open the file in question.
- A lack of user awareness about the risks involved in opening unsolicited e-mails may result in a virus infection spreading throughout your organisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.3.1 Controls against malicious software

Policy 060110
Responding to Virus Incidents

SUGGESTED POLICY STATEMENT

"The threat posed by the infiltration of a virus is high, as is the risk to the organisation's systems and data files. Formal procedures for responding to a virus incident are to be developed, tested and implemented. Virus Incident response must be regularly reviewed and tested."

EXPLANATORY NOTES

Despite general awareness and technical safeguards, some viruses nevertheless enter and infect the organisation's systems.
Dealing with a virus in a professional and planned way reduces both its impact and its spread throughout the organisation and beyond.

Information Security issues to be considered when implementing your policy include the following:

- A failure to respond appropriately to a virus incident can **rapidly** result in multiple systems failures and continued infection.
- Following a restore from backup, and despite having successfully 'quarantined' and applied vaccine to a file known to be infected with a virus, the infected file may be restored in error, and possibly cause more damage.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3.1	Reporting security incidents
8.1.3	Incident management procedures
8.3.1 (g)/(h)	Controls against malicious software

Policy 060111
Installing Virus Scanning Software

SUGGESTED POLICY STATEMENT

"Anti Virus software must be chosen from a proven leading supplier."

EXPLANATORY NOTES

The development of anti-virus software is a highly technical and specialised area. Consequently, you should select your product with care.

Information Security issues to be considered when implementing your policy include the following:

- Inappropriate selection of anti-virus software leaves your organisation with inadequate protection.
- Because anti-virus definitions (the vaccine) are always retrospective, the selection of a brand leader should be carefully considered, as speed is critical.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.3.1 Controls against malicious software

CHAPTER 07
COMPLYING WITH LEGAL AND POLICY REQUIREMENTS

Sub-Chapter 01
Complying with Legal Obligations

Policy 070101	**Being Aware of Legal Obligations**
Policy 070102	**Complying with the Data Protection Act or Equivalent**
Policy 070103	**Complying with General Copyright Legislation**
Policy 070104	**Complying with Database Copyright Legislation**
Policy 070105	**Complying with Copyright and Software Licensing Legislation**
Policy 070106	**Legal Safeguards against Computer Misuse**

Policy 070101
Being Aware of Legal Obligations

SUGGESTED POLICY STATEMENT

"Persons responsible for Human Resources Management are to ensure that all employees are fully aware of their legal responsibilities with respect to their use of computer based information systems and data. Such responsibilities are to be included within key staff documentation such as Terms and Conditions of Employment and the Organisation Code of Conduct."

EXPLANATORY NOTES

Awareness of legal aspects of using computer based information systems is important so that users do not inadvertently contravene legal requirements. Familiarity with relevant legal requirements to your duties and functions should be a requirement of your organisation's Information Security Policy.

Information Security issues to be considered when implementing your policy include the following:

- An absence of published guidelines relating to the legal aspects of using information systems may result in staff failing to comply with the law - leading to prosecution.
- Changes in the law may result in your organisation unintentionally committing an offence.
- The Terms and Conditions of Employment may not have stipulated that the Organisation Code of Conduct must be observed. This could result in the inability to bring disciplinary action against staff found to be in contravention.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.4 Terms and conditions of employment
12.1.1 Identification of applicable legislation

Policy 070102
Complying with the Data Protection Act or Equivalent

SUGGESTED POLICY STATEMENT

"The organisation intends to fully comply with the requirements of Data Protection legislation in so far as it directly affects the organisation's activities."

EXPLANATORY NOTES

Data protection legislation normally covers all types of information which may be either in electronic form or held as manual records. The legislation normally relates to the protection of the rights of individual persons. In many countries it also covers medical records although increasingly this type of information is governed by separate legislation. Internationally, Data Protection has become an important issue. This policy covers its relevance to staff and third parties.

Information Security issues to be considered when implementing your policy include the following:

- If your staff are unaware of the principles of data protection, they may break the law without realising it.
- You are normally required to respond to legitimate enquiries from persons about whom you hold information. Failure to do so can result in legal action.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.4 Data protection and privacy of personal information

Policy 070103
Complying with General Copyright Legislation

SUGGESTED POLICY STATEMENT

"Persons responsible for Human Resources Management are to prepare guidelines to ensure that all employees are aware of the key aspects of Copyright, Designs and Patents Act legislation (or its equivalent), in so far as these requirements impact on their duties."

EXPLANATORY NOTES

The protection of *copyright* is a global issue; viz. the Copyright, Designs and Patents Act, 1988 of the UK, the Intellectual and Industrial Property Law of Canada, and the USA's Copyright Act of 1976, plus legislation in many other countries which were signatories to the international Berne Convention copyright principles. Infringement of copyright is a criminal matter. The simple act of copying copyrighted material constitutes a breach of the law. Even without selling such copies you risk imprisonment and fines. There are no mitigating circumstances.

Information Security issues to be considered when implementing your policy include the following:

- Lack of familiarity with copyright laws may result in inadvertent breaches of it (e.g. making a spare copy of a computer manual), which potentially leads to legal action.
- A failure to adhere to the legal requirements relating to Software Licencing can result in legal action against the organisation and its Directors.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.2 Intellectual property rights (IPR)

Policy 070104
Complying with Database Copyright Legislation

SUGGESTED POLICY STATEMENT

"Persons responsible for Human Resources Management are to prepare guidelines to ensure that all employees are aware of the key aspects of Copyright and Rights in Databases Regulations legislation (or its equivalent), in so far as these requirements impact on their duties."

EXPLANATORY NOTES

In many countries there is legislation covering the protection of information copyrights held in databases. This policy gives a brief outline of copyright, owner rights and user rights, both for online and paper based databases.
A contractual agreement setting out what can and cannot be done to a database is a way of minimising the risk of legal action by users or owners of databases.

Information Security issues to be considered when implementing your policy include the following:

- A database owned by your organisation that is not protected by contractual agreements may expose your organisation to possible ownership disputes.
- Lack of knowledge of database rights regulations could mean that a database which your organisation has compiled from various sources, infringes several copyrights.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.2 Intellectual property rights (IPR)

Policy 070105
Complying with Copyright and Software Licensing Legislation

SUGGESTED POLICY STATEMENT

"Persons responsible for Human Resources Management are to prepare guidelines to ensure that all employees are aware of the key aspects of Software Copyright and Licensing legislation, in so far as these requirements impact on their duties."

EXPLANATORY NOTES

All industrialised countries have specific legislation governing intellectual property rights and software licencing. This policy looks at copyright and software licensing issues from a legal perspective.

Copying and distributing software is illegal, unless permission is expressly granted by the owner of the software.

Information Security issues to be considered when implementing your policy include the following:

- Unless your organisation has a licence from the owner of the software to copy and distribute computer software, copying is illegal.
- Software may be copied and distributed across your computer network in contravention of the licensing agreement. This illegal activity threatens your organisation's integrity and may result in legal action.
- Use of unlicensed software by contractors or consultants on your premises could result in legal action being taken against your organisation.
- If required, you must be able to produce the licences for inspection, or potentially risk a fine and possible public embarrassment.

N.B. To enforce the position, some organisations have voluntarily 'opened their doors' to inspectors from the Federation Against Software Theft (FAST) to confirm both their software legality and their procedures for preventing infringement of the law.

- Where a legitimate licence has been purchased, lack of internal controls can result in the maximum number of permitted users being exceeded. A single excess copy places your organisation at risk from prosecution under copyright laws.
- You should always obtain legal advice on the local requirements and legislation governing intellectual property rights and software licencing.

- Resale of old or redundant computer equipment can result in an infringement of the copyright law, as software licence agreements may not be transferable.
- If 'shareware' software, downloaded from public networks (e.g. the Internet), is used beyond its evaluation period (as stated within the *EULA*) infringement of the terms of the licence is likely.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.2 Intellectual property rights (IPR)

Policy 070106
Legal Safeguards against Computer Misuse

SUGGESTED POLICY STATEMENT

"Persons responsible for Human Resources Management are to prepare guidelines to ensure that all employees are aware of the key aspects of Computer Misuse legislation (or its equivalent), in so far as these requirements impact on their duties."

EXPLANATORY NOTES

Computer misuse policy should take into consideration the following:

1) Unauthorised access to computer systems which covers anything from harmless exploration, to hacking for access to specific data.
2) Unauthorised access to computer systems with the intent of using the information accessed for a further offence, e.g. extortion.
3) Offences are those of unauthorised access to computer systems with the intent of modifying the contents of the computer.

Information Security issues to be considered when implementing your policy include the following:

- Persons who store, copy or distribute illegal or offensive material may be committing an offence.
- Authority to access the organisation's systems may be assumed, because unauthorised access is not expressly prohibited.
- System software messages, displayed prior to authenticated logon, can be construed as an invitation to use the computer system, and potentially encourage unauthorised access.
- Pre-login information screen messages which describe the services or options available to users once they have logged in, can increase the risk of further attempts to access your information systems.
- System capacity and performance can deteriorate when unauthorised programs are run, possibly resulting in delays to critical business processing.
- Staff using the organisation's computer systems to process private data (e.g. mailing lists, creating a Web site, etc.) may not only be wasting time and resources, but additionally be committing offences.
- Where the terms and conditions of third party access to your organisations' systems are not covered by the associated contractual agreements between the

respective organisations, your organisation is exposed to possible prosecution in the event of computer misuse.

- Legal advice should always be obtained when considering organisational policy on computer misuse.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.5 Prevention of misuse of information processing facilities

Sub-Chapter 02
Complying with Policies

Policy 070201 **Managing Media Storage and Record Retention**

Policy 070202 **Complying with Information Security Policy**

Policy 070201
Managing Media Storage and Record Retention

SUGGESTED POLICY STATEMENT

"The organisation will maintain a suitable archiving and record retention procedure."

EXPLANATORY NOTES

Retention of records and storage media is often a legal requirement. This topic looks at the issue of access to archived data being difficult or impossible, and thereby restricting your organisation's ability to meet its legal obligations.

It is important to be aware of the pitfalls posed by obsolete or redundant storage technologies, limiting your organisation's ability to access data.

Information Security issues to be considered when implementing your policy include the following:

- Where your primary business records are inadequately stored and safeguarded, they are susceptible to modification, deletion or corruption, thereby destroying the *integrity* of the contents. This could threaten the organisation's ability to meet any legal / regulatory obligations regarding the retention of records.
- You may not be able to read the information stored on 'old' media (e.g. tape cartridges) because your organisation has adopted more modern technologies. This could have serious implications for your organisation.

N.B. This is a real risk that has yet to be fully quantified. With the accelerating evolution of operating systems, processor technology, and software, it is uncertain which of the late 20th century and early 21st century 'standards', will still be in use, say, in 10 years time if the need arises to restore pre-2000 data files.

- The lack of an adequate retention policy for different categories of information may mean that you do not meet regulatory or statutory requirements, and could potentially result in legal action.
- Lack of knowledge of the regulations for the acquisition and use of cryptographic systems may lead to prosecution under a number of countries' laws.
- Following expiry of the agreed retention period, the data should be made available for either destruction or for possible further retention, according to business need. However, further retention could contravene *Data Protection Act* principles.

- If encryption has been used to protect sensitive records, and the controls over the cryptographic keys is reduced, future access to the material may be jeopardised.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.3 Safeguarding of organisational records

Policy 070202
Complying with Information Security Policy

SUGGESTED POLICY STATEMENT

"All employees are required to fully comply with the organisation's Information Security policies. The monitoring of such compliance is the responsibility of management."

EXPLANATORY NOTES

Compliance with your organisation's Information Security Policy is mandatory. This topic discusses ways of ensuring that compliance is achieved and failures to comply are actioned.

The compliance monitoring process could lead to resentment among staff, unless it is handled sensitively.

Information Security issues to be considered when implementing your policy include the following:

- Complacency over Information Security Policy compliance may inadvertently expose your organisation to legal action.
- The integrity of an Information Security audit can be threatened where software tools (for probing and analysis) are accessible to unauthorised users who might corrupt / modify the results. See *Access Control*.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.4 Terms and conditions of employment
12.2.1 Compliance with security policy

Sub-Chapter 03
Avoiding Litigation

Policy 070301 **Safeguarding against Libel and Slander**

Policy 070302 **Using Copyrighted Information from the Internet**

Policy 070303 **Sending Copyrighted Information Electronically**

Policy 070304 **Using Text directly from Reports, Books or Documents**

Policy 070301
Safeguarding against Libel and Slander

SUGGESTED POLICY STATEMENT

"Employees are prohibited from writing derogatory remarks about other persons or organisations."

EXPLANATORY NOTES

Casual comments in e-mails relating to individuals or rival companies may be construed as defamatory - even if the comments are valid.

This policy discusses ways of discouraging the publication of this type of material. The legal consequences for publishing potentially defamatory material on an open access medium, such as the Internet, can be severe.

Information Security issues to be considered when implementing your policy include the following:

- A casual comment posted through your systems, to an Internet *News Group* about a business competitor could result in legal action being taken against your organisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.1 Identification of applicable legislation
12.1.5 Prevention of misuse of information processing facilities

Policy 070302
Using Copyrighted Information from the Internet

SUGGESTED POLICY STATEMENT

"Information from the Internet or other electronic sources may not be used without authorisation from the owner of the copyright."

EXPLANATORY NOTES

Information obtained via the Internet may be covered by copyright law which must be observed.

Information Security issues to be considered when implementing your policy include the following:

- The organisation is open to litigation if data you hold or use in your system is copyrighted by a third party.
- The organisation may lose the use of information copyrighted by a third party.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.2 Intellectual property rights (IPR)

Policy 070303
Sending Copyrighted Information Electronically

SUGGESTED POLICY STATEMENT

"Information from the Internet or other electronic sources may not be retransmitted without permission from the owner of the copyright."

EXPLANATORY NOTES

The information supplied to you via the Internet is still covered by copyright law and anything you do with the data must observe it.

Information Security issues to be considered when implementing your policy include the following:

- Copyright owners may take you to court if you send information electronically without permission (e-mail and web based links).

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.2 Intellectual property rights (IPR)

Policy 070304
Using Text directly from Reports, Books or Documents

SUGGESTED POLICY STATEMENT

"Text from reports, books or documents may not be reproduced or reused without permission from the copyright owner."

EXPLANATORY NOTES

When you use text directly from other people's work the copyright issues are easy to deal with. Pay for the use of the work. The greater risk concerns the validity and integrity of the data. The information may be wrong or taken out of context.

Information Security issues to be considered when implementing your policy include the following:

- Your information may be corrupted or have been modified using incorrect data.
- You are legally liable for any breach of copyright law. You may be taken to court and fined or penalised.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.2 Intellectual property rights (IPR)

Sub-Chapter 04
Other Legal Issues

Policy 070401
Recording Evidence of Incidents (Information Security)

SUGGESTED POLICY STATEMENT

"All employees are to be aware that evidence of Information Security incidents must be formally recorded and retained and passed to the appointed Information Security Officer."

EXPLANATORY NOTES

Evidence is collected in two cases, either because there has already been a breach of the law, or a breach is thought to be imminent. If you believe there has been a breach of Information Security, refer to *Detecting and Responding to Information Security Incidents* for guidelines. Where the breach has not yet taken place, but you suspect it may, it is important that any evidence being collected is admissible. See *Admissible Evidence*. **N.B.** Organisations should **always** seek legal advice concerning the admissibility of any evidence.

Information Security issues to be considered when implementing your policy include the following:

- Where the evidence produced is not considered admissible, any possible legal case may be dismissed, and other forms of disciplinary action may fail.
- Lack of continuity and completeness of evidence can compromise the legal position.
- Where proof that the evidence has not been 'modified' is unavailable or unsatisfactory, the integrity of the evidence may be in doubt.
- Where there is no written evidence that the perpetrator was aware of any access restrictions to the various systems, this can scupper any legal redress.
- Notwithstanding the possible admissibility of the evidence collected, where no procedures exist for the collection, storage and safekeeping of such evidence, it may be deemed inadmissible.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3.1 Reporting security incidents
9.7.1 Event logging
9.7.2 Monitoring system use
12.1.7 Collection of evidence

Policy 070402
Renewing Domain Name Licences – Web Sites

SUGGESTED POLICY STATEMENT

"Registered domain names, whether or not actually used for the organisation's Web sites, are to be protected and secured in a similar manner to any other valuable asset of the organisation."

EXPLANATORY NOTES

The domain name that you use for your Web site and Internet activities is how you maintain your presence on the web. If you lose control of this name then all publicity and previous marketing activities are wasted. Effectively, you may lose all business and Internet based information which you may have obtained via that domain.

Information Security issues to be considered when implementing your policy include the following:

- Your domain name ownership may be challenged by the registered trademark owner.
- Your domain name registration lapses by mistake, allowing a competitor to 'take the name'.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.2 Intellectual property rights (IPR)

Policy 070403
Insuring Risks

SUGGESTED POLICY STATEMENT

"A re-assessment of the threats and risks involved relating to the organisation's business activities must take place periodically to ensure that the organisation is adequately insured at all times."

EXPLANATORY NOTES

All aspects of your systems and their information environment should be properly insured to cover actual loss and related loss of profits cover.

Information Security issues to be considered when implementing your policy include the following:

- A failure to establish what is insurable against loss will result in financial loss.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

Introduction	How to establish security requirements Assessing security risks
12.1.3	Safeguarding of organisational records

Policy 070404
Recording Telephone Conversations

SUGGESTED POLICY STATEMENT

"All parties are to be notified in advance whenever conversations are being recorded."

EXPLANATORY NOTES

Telephone conversations are recorded by companies for several reasons: legal, monitoring, staff training, and recording details of orders and requests. They may be stored as voice recordings or transcribed into other media. Telephone conversations are only to be recorded when all parties have been notified in advance that the conversation is being recorded.

Information Security issues to be considered when implementing your policy include the following:

- Confidential Telephone call recording or transcripts of client information may be leaked to a third party.
- Recorded data may be accessed without authorisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.7 Other forms of information exchange
12.1.1 Identification of applicable legislation

CHAPTER 08
PLANNING FOR BUSINESS CONTINUITY

Sub-Chapter 01 Business Continuity Management (BCP)

Sub-Chapter 01
Business Continuity Management (BCP)

Policy 080101	**Initiating the BCP Project**
Policy 080102	**Assessing the BCP Security Risk**
Policy 080103	**Developing the BCP**
Policy 080104	**Testing the BCP**
Policy 080105	**Training and Staff Awareness on BCP**
Policy 080106	**Maintaining and Updating the BCP**

Policy 080101
Initiating the BCP Project

SUGGESTED POLICY STATEMENT

"Management are required to initiate a Business Continuity Plan."

EXPLANATORY NOTES

Business Continuity Planning (BCP) is essential for the continuation of key business services, in the event of an unexpected occurrence which seriously disrupts the business process.

The BCP Project needs to be initiated and formally approved and committed to by the Board or Governing body of the organisation.

Information Security issues to be considered when implementing your policy include the following:

- Lack of Board or top management commitment to formal BCP development is likely to result in an inadequate process.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

11.1.1 Business continuity management process
11.1.4 Business continuity planning framework

Policy 080102
Assessing the BCP Security Risk

SUGGESTED POLICY STATEMENT

"Management is to undertake a formal risk assessment in order to determine the requirements for a Business Continuity Plan."

EXPLANATORY NOTES

Business Continuity Planning (BCP) is essential for the continuation of key business services, in the event of an unexpected occurrence which seriously disrupts the business process.

BCP - Risk Assessment analyses the nature of such unexpected occurrences, their potential impact, and the likelihood of these occurrences becoming serious incidents.

Information Security issues to be considered when implementing your policy include the following:

- Even where a formal BCP project has been initiated, if the allocated financial and human resources are insufficient, the resultant plan is unlikely to succeed.
- Underestimating the short and medium term impact of a Security Incident can result in an inappropriate level of response towards building a suitable BCP.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

11.1.2 Business continuity and impact analysis
11.1.4 Business continuity planning framework

Policy 080103
Developing the BCP

SUGGESTED POLICY STATEMENT

"Management is to develop a Business Continuity Plan which covers all essential and critical business activities."

EXPLANATORY NOTES

Business Continuity Planning (BCP) is essential for the continuation of key business services in the event of an unexpected occurrence which seriously disrupts the business process.

The Business Continuity Plan is a project plan which is likely to be complex and detailed. Irrespective of the nature of your particular organisation, it will probably contain a series of critical actions which will lead to the return of normal operations.

Information Security issues to be considered when implementing your policy include the following:

- When the need arises to trigger the BCP, but:

  - it does not exist, or
  - is untested, or
  - is non viable, or
  - fails when activated.....

  The organisation's operations may not be able to recover - **ever**.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

11.1.3 Writing and implementing continuity plans
11.1.4 Business continuity planning framework

Policy 080104
Testing the BCP

SUGGESTED POLICY STATEMENT

"The Business Continuity Plan is to be periodically tested to ensure that the management and staff understand how it is to be executed."

EXPLANATORY NOTES

Business Continuity Planning (BCP) is essential for the continuation of key business services in the event of an unexpected occurrence which seriously disrupts the business process.

Testing your organisation's Business Continuity Plan (BCP) assesses its viability, and ensures your staff are conversant with the proposals.

Information Security issues to be considered when implementing your policy include the following:

- Where the BCP Testing does not reproduce authentic conditions, the value of such testing is limited.
- A failure to analyse the BCP Test Plan results will likely detract from the value of the test.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

11.1.4 Business continuity planning framework
11.1.5 Testing, maintaining and re-assessing business continuity plans

Policy 080105
Training and Staff Awareness on BCP

SUGGESTED POLICY STATEMENT

"All staff must be made aware of the Business Continuity Plan and their own respective roles."

EXPLANATORY NOTES

Business Continuity Planning (BCP) is essential for the continuation of key business services in the event of an unexpected occurrence which seriously disrupts the business process.

If a Business Continuity Plan (BCP) is to be executed successfully, all personnel must not only be aware that the plan exists, but also know its contents, together with the duties and responsibilities of each party.

Information Security issues to be considered when implementing your policy include the following:

- Even a BCP that is tested can fail if personnel are insufficiently familiar with its contents.
- Where BCP becomes divorced from people's perception of realistic risk, a sense of apathy can de-prioritise their need for participation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

11.1.4 Business continuity planning framework
11.1.5 Testing, maintaining and re-assessing business continuity plans

Policy 080106
Maintaining and Updating the BCP

SUGGESTED POLICY STATEMENT

"The Business Continuity Plan is to be kept up to date and re-tested periodically."

EXPLANATORY NOTES

Business Continuity Planning (BCP) is essential for the continuation of key business services in the event of an unexpected occurrence which seriously disrupts the business process.

The maintaining and updating of the Business Continuity Plan (BCP) is critical if its successful execution is to be relied upon.

Information Security issues to be considered when implementing your policy include the following:

- Where the updates to the BCP have not probed the implications and underlying assumptions resulting from changes, the execution of the BCP may be flawed.
- Where the BCP is not being updated periodically, its fitness for purpose may be questionable.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

11.1.4 Business continuity planning framework
11.1.5 Testing, maintaining and re-assessing business continuity plans

CHAPTER 09
ADDRESSING PERSONNEL ISSUES RELATING TO SECURITY

Sub-Chapter 01
Contractual Documentation

Policy 090101	**Preparing Terms and Conditions of Employment**
Policy 090102	**Employing / Contracting New Staff**
Policy 090103	**Contracting with External Suppliers / other Service Providers**
Policy 090104	**Using Non Disclosure Agreements (Staff and Third Party)**
Policy 090105	**Misuse of Organisation Stationery**
Policy 090106	**Lending Keys to Secure Areas to Others**
Policy 090107	**Lending Money to Work Colleagues**
Policy 090108	**Complying with Information Security Policy**
Policy 090109	**Establishing Ownership of Intellectual Property Rights**
Policy 090110	**Employees' Responsibility to Protect Confidentiality of Data**

Policy 090101
Preparing Terms and Conditions of Employment

SUGGESTED POLICY STATEMENT

"The Terms and Conditions of Employment of this organisation are to include requirements for compliance with Information Security."

EXPLANATORY NOTES

The Terms and Conditions of Employment specify the particulars of the employment relationship between an employer and employee. All such documents usually cover certain basic issues, but their content may also vary because what is deemed necessary for inclusion depends on the type of organisation, the position, and so forth. Standard contracts of employment are re-drafted from time to time to ensure that they keep up with the changing times. Increasingly, the issue of Information Security is being recognised as one that should be expressly addressed in modern contracts of employment.

Information Security issues to be considered when implementing your policy include the following:

- Where individual job descriptions and duties make no reference to Information Security other than for technical people, staff may be under the mistaken impression that they have no responsibility for Information Security.
- Where the Terms and Conditions of Employment do not incorporate the security requirements for the use of information systems, your organisation could possibly suffer damage with minimal legal redress against the individual(s) concerned.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.1 Including security in job responsibilities
6.3.5 Disciplinary process

Policy 090102
Employing / Contracting New Staff

SUGGESTED POLICY STATEMENT

"New employees' references must be verified, and the employees must undertake to abide by the organisation's Information Security policies."

EXPLANATORY NOTES

Employers should protect themselves against hiring individuals who are ill suited to the demands of the job. Such employees will be given access to the organisation's Information Systems, and therefore the resultant Information Security risks need to be addressed.

Information Security issues to be considered when implementing your policy include the following:

- Poor pre-employment screening methods can lead to employment of a person with unsuitable or even possibly fictitious credentials.
- If new staff are unaware of your Information Security Policies your organisation may suffer damage with possibly little legal redress against the individual(s) concerned.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.2 Personnel screening and policy

Policy 090103
Contracting with External Suppliers / other Service Providers

SUGGESTED POLICY STATEMENT

"All external suppliers who are contracted to supply services to the organisation must agree to follow the Information Security policies of the organisation. An appropriate summary of the Information Security Policies must be formally delivered to any such supplier, prior to any supply of services."

EXPLANATORY NOTES

Adequate security constraints may be in force for employees and contractors, but those same levels of safeguard maybe overlooked when dealing with third parties, such as hardware and software suppliers, consultants and other service providers.

Information Security issues to be considered when implementing your policy include the following:

- Where third party agreements do not refer to your Information Security Policy, you may have difficulty in making a case if the breach of security should only become evident after the contract with the third party is completed.
- Where a contract with an external service provider does not refer to the Information Security Policies and Standards of your organisation, your information is at greater risk as their standards and safeguards are likely to differ.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.3 Security requirements in outsourcing contracts

Policy 090104
Using Non Disclosure Agreements (Staff and Third Party)

SUGGESTED POLICY STATEMENT

"Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is classified as Proprietary (or above)."

EXPLANATORY NOTES

It is common practice to use a *Non Disclosure Agreement* or NDA as a legally enforceable means of redress for the case that a third party may inappropriately communicate confidential information covered by the NDA to a non authorised party. All staff should sign contracts of employment with non disclosure clauses duly inserted.

Information Security issues to be considered when implementing your policy include the following:

- A failure to have your staff sign individual employment contracts with non disclosure clauses, may result in your trade secrets being divulged or your organisation's ideas developed by others.
- Where NDAs are not agreed and signed with third parties who have access to your information systems and projects, unguarded conversations may result in sensitive information being divulged to a competitor.
- When staff resign, retire or are asked to leave, a failure to have obtained signed non disclosure clauses, with indefinite validity, may leave the organisation exposed to the risk that confidential information may subsequently be leaked.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.3 Confidentiality agreements

Policy 090105
Misuse of Organisation Stationery

SUGGESTED POLICY STATEMENT

"The organisation's letter-headed notepaper, printed forms and other documents are to be handled securely to avoid misuse."

EXPLANATORY NOTES

The use of organisation stationery often authenticates the validity of the information contained on it. Its misuse can breach security.

Information Security issues to be considered when implementing your policy include the following:

- Your organisation's image and reputation could be irreparably damaged by the fraudulent use of the organisation's stationery.
- Where confidential information is obtained and modified by unauthorised individuals using stolen organisation stationery, such forgery can result in commercial damage and legal proceedings.
- The organisation's office resources may be stolen through the unauthorised use of order forms and other stationery.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.4 Terms and conditions of employment

Policy 090106
Lending Keys to Secure Areas to Others

SUGGESTED POLICY STATEMENT

"The lending of keys, both physical or electronic, is prohibited. This requirement is also to be noted in employment contracts."

EXPLANATORY NOTES

The use of keys, whether physical and electronic, to access secure areas is to be policed strictly because the possession of keys to an area is often taken as permission to enter it. Keys should be issued to authorised staff only.

Information Security issues to be considered when implementing your policy include the following:

- The confidentiality of your information will be compromised by unauthorised persons accessing secure areas with borrowed keys / passes, despite the fact the action was possibly well intentioned.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.4 Terms and conditions of employment

Policy 090107
Lending Money to Work Colleagues

SUGGESTED POLICY STATEMENT

"Lending money to work colleagues is strongly discouraged."

EXPLANATORY NOTES

This is a serious matter and should be strongly discouraged.

Information Security issues to be considered when implementing your policy include the following:

- Lending money to work colleagues can lead to friction and bad atmospheres when the money is not repaid.
- This activity can create unhealthy pressures thereby potentially creating collusion situations.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.2.1 Information security education and training

Policy 090108
Complying with Information Security Policy

SUGGESTED POLICY STATEMENT

"All employees must comply with the Information Security Policies of the organisation. Any Information Security incidents resulting from non-compliance will result in immediate disciplinary action."

EXPLANATORY NOTES

All employees are required to comply with all Information Security Policies.

Information Security issues to be considered when implementing your policy include the following:

- Where non compliance with the organisation's Information Security Policy results in loss, damage or breach of confidentiality, appropriate action should be taken.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.1 Including security in job responsibilities
6.3.5 Disciplinary process
12.2.1 Compliance with security policy

Policy 090109
Establishing Ownership of Intellectual Property Rights

SUGGESTED POLICY STATEMENT

"All employees and third party contractors are to sign a formal undertaking regarding the intellectual property rights of work undertaken during their terms of employment / contract respectively."

EXPLANATORY NOTES

All Intellectual Property Rights over work done by employees of the organisation as part of their normal or other duties is to be owned by the organisation. If the organisation wishes to own the Intellectual Property Rights over work done by third parties or contractors, then it must ensure that the agreement or contract with the third party covers this issue.

Information Security issues to be considered when implementing your policy include the following:

- Where an employee does not recognise and respect the Intellectual Property Rights over their work created for the organisation, they may be tempted for personal gain.
- Where the organisation does not make it clear that it **owns** all work created by third party contractors for, and on behalf of the organisation, it could suffer financial loss were a legal claim to be made.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.1 Including security in job responsibilities
12.1.2 Intellectual property rights (IPR)

Policy 090110
Employees' Responsibility to Protect Confidentiality of Data

SUGGESTED POLICY STATEMENT

"All employees are required to sign a formal undertaking concerning the need to protect the confidentiality of information, both during and after contractual relations with the organisation."

EXPLANATORY NOTES

A key aspect of any Information Security process is the maintenance of confidentiality of information and data.

Information Security issues to be considered when implementing your policy include the following:

- Employees, whether intentionally or not, may release confidential information to persons outside the organisation.
- Employees, usually trying to make a good impression with their subsequent employer, may be tempted to take confidential information with them when they leave the organisation's employment.
- Employees may not understand the risks and potential consequences of releasing sensitive information to unauthorised persons.
- Employees may openly discuss confidential issues in the work place, that have, or should have, restricted access.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.1 Including security in job responsibilities
12.1.4 Data protection and privacy of personal information

Sub-Chapter 02
Confidential Personnel Data

Policy 090201
Respecting Privacy in the Workplace

SUGGESTED POLICY STATEMENT

"Notwithstanding the organisation's respect for employee's privacy in the workplace, it reserves the right to have access to all information created and stored on the organisation's systems."

EXPLANATORY NOTES

Recent Human Rights legislation has established the fundamental need to respect a person's privacy. However, whether or not such rights become enforceable will greatly depend upon whether the employee has reasonable grounds to contend that certain information received, stored and / or created on the employer's systems may be reasonably considered as 'private'. Your Information Security Policy must be clear about this.

Information Security issues to be considered when implementing your policy include the following:

- Where the monitoring of employee activity is **perceived** as intrusive and / or excessive and in contravention of the law, legal proceedings could result in fines and other penalties for your organisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.4 Terms and conditions of employment
12.1.4 Data protection and privacy of personal information

Policy 090202
Handling Confidential Employee Information

SUGGESTED POLICY STATEMENT

"All employee data is to be treated as strictly confidential and made available to only properly authorised persons."

EXPLANATORY NOTES

Employee information should not be disclosed to unauthorised persons. The disclosure of this type of information may be covered by data privacy legislation.

Information Security issues to be considered when implementing your policy include the following:

- Employee data which has not been held securely could be stolen or illegally modified .
- If limits to access and distribution are not defined, confidential employee information may be accessed without authorisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.4 Data protection and privacy of personal information

Policy 090203
Giving References on Staff

SUGGESTED POLICY STATEMENT

"Only authorised personnel may give employee references."

EXPLANATORY NOTES

The preparing of references is a specialised process and should only be undertaken by properly trained and authorised persons. When giving references ensure that you are aware of who is requesting the information and why.

Information Security issues to be considered when implementing your policy include the following:

- Passing inaccurate or inappropriate personal reference details to third parties may result in liability claims.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.2 Personnel screening and policy
12.1.4 Data protection and privacy of personal information

Policy 090204
Checking Staff Security Clearance

SUGGESTED POLICY STATEMENT

"All staff must have previous employment and other references carefully checked."

EXPLANATORY NOTES

A large number of security breaches are initiated by dishonest or aggrieved staff. Care must be taken in assigning security clearance levels to staff members and also in checking the validity of their security clearance authorities.

Information Security issues to be considered when implementing your policy include the following:

- Confidential systems may be penetrated by an employee who was wrongly granted authority to access sensitive information or data.
- Confidential data may be accessed by unauthorised staff because their security rating has not been kept in line with any changes in their job.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.2 Personnel screening and policy

Policy 090205
Sharing Employee Information with Other Employees

SUGGESTED POLICY STATEMENT

"Employee data may only be released to persons specifically authorised to receive this information."

EXPLANATORY NOTES

Employee data is privileged and should not be divulged to other employees unless authorised.

Information Security issues to be considered when implementing your policy include the following:

- Leaked employee information is not only likely to cause distress, such a breach may result in legal proceedings.
- An Employee's personal details may be passed to outsiders via a staff member; again breaching confidentiality.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.4 Data protection and privacy of personal information

Policy 090206
Sharing Personal Salary Information

SUGGESTED POLICY STATEMENT

"Employees are discouraged from sharing personal salary details and other terms and conditions with other members of staff."

EXPLANATORY NOTES

Many security breaches are caused by disgruntled staff. Salary details constitute sensitive confidential organisation information and should be treated accordingly. Sharing them is the quickest way to make colleagues disgruntled.

Information Security issues to be considered when implementing your policy include the following:

- Confidential salary data is passed to unauthorised staff members.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.2.1 Information security education and training

Sub-Chapter 03
Personnel Information Security Responsibilities

Policy 090301	**Using the Internet in an Acceptable Way**
Policy 090302	**Keeping Passwords / PIN Numbers Confidential**
Policy 090303	**Sharing Organisation Information with Other Employees**
Policy 090304	**Using E-Mail and Postal Mail Facilities for Personal Reasons**
Policy 090305	**Using Telephone Systems for Personal Reasons**
Policy 090306	**Using the Organisation's Mobile Phones for Personal Use**
Policy 090307	**Using Organisation Credit Cards**
Policy 090308	**Signing for the Delivery of Goods**
Policy 090309	**Signing for Work done by Third Parties**
Policy 090310	**Ordering Goods and Services**
Policy 090311	**Verifying Financial Claims and Invoices**
Policy 090312	**Approving and Authorisation of Expenditure**
Policy 090313	**Responding to Telephone Enquiries**
Policy 090314	**Sharing Confidential Information with Family Members**
Policy 090315	**Gossiping and Disclosing Information**
Policy 090316	**Spreading Information through the Office 'Grape Vine'**

Policy 090317 Playing Games on Office Computers

Policy 090318 Using Office Computers for Personal Use

Policy 090301
Using the Internet in an Acceptable Way

SUGGESTED POLICY STATEMENT

"Employees may not use the organisation's systems to access or download material from the Internet which is inappropriate, offensive, illegal, or which jeopardises security. All Internet use must be for business related purposes."

EXPLANATORY NOTES

If your organisation's Information Security Policies do not explicitly state what is deemed acceptable, it may be hard, or impossible to invoke any form of disciplinary action against those involved. Your Information Security Policy must be clear about this.

Information Security issues to be considered when implementing your policy include the following:

- The following examples of Internet access not only detract from business efficiency, some can even result in legal and criminal proceedings, which will almost certainly damage the organisation.

  1. Downloading of pornographic material from Web sites
  2. Playing games and using 'Chat Rooms'.
  3. Subscribing and contributing to *News Groups* using the corporate Internet address and *signature*.
  4. Sending and receiving personal correspondence by e-mail, the volume and content of which is deemed as excessive and / or inappropriate.
  5. Excessive 'surfing' of Web sites during business hours for personal reasons.
  6. Retrieval and distribution to other staff of offensive 'joke of the day' e-mails
  7. The use and abusive of office equipment for the storage and printing of inappropriate material e.g. large pictures / images.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3.5 Disciplinary process
12.1.5 Prevention of misuse of information processing facilities

Policy 090302
Keeping Passwords / PIN Numbers Confidential

SUGGESTED POLICY STATEMENT

"All personnel must treat passwords as private and highly confidential. Non-compliance with this policy could result in disciplinary action."

EXPLANATORY NOTES

This topic is concerned with the responsibilities of staff with regard to all forms of access passwords - including PIN numbers.

Information Security issues to be considered when implementing your policy include the following:

- Information may be disclosed without authorisation, because passwords have been compromised or not kept confidential.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3.5 Disciplinary process
12.1.5 Prevention of misuse of information processing facilities

Policy 090303
Sharing Organisation Information with Other Employees

SUGGESTED POLICY STATEMENT

"Confidential information should be shared only with other authorised persons."

EXPLANATORY NOTES

Organisation information has its own individual levels of sensitivity, and as such must not be divulged to staff that do not have authorisation to access that information.

Information Security issues to be considered when implementing your policy include the following:

- Confidential organisation data may be at risk because authorised staff members are not fully aware of the data's context.
- Confidential organisation data may be at risk through access by unauthorised staff members.
- Confidential data may be compromised if given to unauthorised staff.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.3 Confidentiality agreements
6.1.4 Terms and conditions of employment

Policy 090304
Using E-Mail and Postal Mail Facilities for Personal Reasons

SUGGESTED POLICY STATEMENT

"The use of e-mail for personal use is discouraged, and should be kept to a minimum. Postal mail may be used for business purposes only."

EXPLANATORY NOTES

All organisation mailing systems, whether conventional or electronic, should be under appropriate control. If the organisation decides to allow minimal personal use of the e-mailing system then it should also require that each use should be authorised.

Information Security issues to be considered when implementing your policy include the following:

- Confidential material may be sent out via un-monitored mail systems.
- A lack of defined policy on private use of e-mail systems may lead to a loss of resources (bandwidth and data).
- Excessive sending of personal e-mails may lock up the network and the system.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.5 Prevention of misuse of information processing facilities

Policy 090305
Using Telephone Systems for Personal Reasons

SUGGESTED POLICY STATEMENT

"Personal calls on the telephone systems are to be minimised and limited to urgent or emergency use only."

EXPLANATORY NOTES

The telephone system is largely forgotten as a threat to security. Handsets are normally on everybody's desk, and the use of a phone does not usually raise a suspicion.

Information Security issues to be considered when implementing your policy include the following:

- A lack of suitable personal use policy for the telephone system may lead to loss or the abuse of information.
- Excessive use of the phone system may not only incur unnecessary costs but also hinder genuine business use.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.5 Prevention of misuse of information processing facilities

Policy 090306
Using the Organisation's Mobile Phones for Personal Use

SUGGESTED POLICY STATEMENT

"The use of the organisation's mobile phones will to be monitored for inappropriate call patterns, unexpected costs, and excessive personal use."

EXPLANATORY NOTES

The private use of organisation supplied mobile phones at work should be discouraged, as outgoing calls should be made via your *PABX* for cost and monitoring reasons. If employee responsibilities warrant the issue of an organisation mobile phone (e.g. sales force) then itemised bills should be reviewed to monitor inappropriate call patterns.

Information Security issues to be considered when implementing your policy include the following:

- Confidential information may be disclosed and misappropriated to unauthorised parties over the phone.
- Confidential information may be discussed in open areas or inappropriate locations (e.g. in airport lounges) and overheard by interested parties.
- Staff should always be notified if their activities may be subject to being monitored from time to time.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.5 Prevention of misuse of information processing facilities

Policy 090307
Using Organisation Credit Cards

SUGGESTED POLICY STATEMENT

"'Company' Credit cards issued to authorised staff remain the responsibility of those employees until the card is returned or cancelled."

EXPLANATORY NOTES

The use of organisation credit cards should be reserved for ad hoc or incidental expenses that do not require a formal purchase order. Certain types of Internet purchases and telephone purchases have to be purchased through credit cards.

Information Security issues to be considered when implementing your policy include the following:

- Where a credit card user authorises payment, spending control may be compromised.
- Confidential organisation credit card details (PIN numbers & account details) could be compromised.
- Passing credit card details to third parties on the Internet can compromise security.
- The security of the company hosting the e-commerce Web site offering credit card purchase, may in doubt.
- Credit cards may be lost or stolen.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.4 Terms and conditions of employment

Policy 090308
Signing for the Delivery of Goods

SUGGESTED POLICY STATEMENT

"Only authorised employees may sign for the receipt of goods. They are to ensure that, by signing for them, they are not considered to be verifying the quality or condition of the goods."

EXPLANATORY NOTES

When goods are delivered to the organisation they should be signed for by the authorised person accepting receipt of the goods.

Information Security issues to be considered when implementing your policy include the following:

- Persons delivering goods may be given access to sensitive areas, threatening your Information Security.
- If there are no guidelines set on the signing for the delivery of goods, the value is questionable.
- A signature could be obtained without the signatory realising exactly what they are signing for.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.2.1 Information security education and training

Policy 090309
Signing for Work done by Third Parties

SUGGESTED POLICY STATEMENT

"Only properly authorised persons may sign for work done by third parties."

EXPLANATORY NOTES

The signature verifies that the work is complete and is part of the *change control process* and also forms part of the *audit trail*. A signature by a technical person may be required in certain circumstances for quality control purposes. Only authorised persons are permitted to sign for work completed by third parties.

Information Security issues to be considered when implementing your policy include the following:

- Persons awaiting a signature for work completed may be given access to sensitive areas, threatening your Information Security.
- Where guidelines on signing for outsourced work are not available, the value is questionable.
- Where the signatory is not authorised, redress may be difficult, especially where the work is subsequently found to be faulty.
- A signature may be obtained on a document without the signatory being aware of exactly what they are signing for.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.2.2 Security requirements in third party contracts

Policy 090310
Ordering Goods and Services

SUGGESTED POLICY STATEMENT

"Only authorised persons may order goods on behalf of the organisation. These goods must be ordered in strict accordance with the organisation's purchasing policy."

EXPLANATORY NOTES

Whether you are ordering from a third party, or they from you, the process of ordering goods can constitute a security risk, because the information given to third parties to process a specific order (credit card details, signatures, etc) could be used elsewhere. See *Using Organisation Credit Cards*.

Information Security issues to be considered when implementing your policy include the following:

- The stated features and performance of the product may not be in accordance with your expectations and could disrupt normal operations if simply introduced into your 'live' operation.
- Under the guise of 'delivering goods', persons with ill intent may gain access to your premises.
- Staff may inadvertently disclose confidential organisation information when ordering goods.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.2.1 Information security education and training

Policy 090311
Verifying Financial Claims and Invoices

SUGGESTED POLICY STATEMENT

"All claims for payment must be properly verified for correctness before payment is effected."

EXPLANATORY NOTES

Invoices and other financial claims on the organisation are to be properly checked, verified and approved before payment.

Information Security issues to be considered when implementing your policy include the following:

- Information on invoices or claims may be inaccurate or totally false.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.2.2 Security requirements in third party contracts

Policy 090312
Approving and Authorisation of Expenditure

SUGGESTED POLICY STATEMENT

"Only authorised persons may approve expenditure or make commitments on behalf of the organisation for future expenditure."

EXPLANATORY NOTES

Expenditure is to be properly authorised in writing before committing to the purchase. Claims for payment are to be properly verified.

Information Security issues to be considered when implementing your policy include the following:

- Changes to expenses claims may conceal on going fraudulent activity.
- A theft may arise through the unauthorised approval of expenditure for work not actually done.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.4 Terms and conditions of employment

Policy 090313
Responding to Telephone Enquiries

SUGGESTED POLICY STATEMENT

"Telephone enquiries for sensitive or confidential information are initially to be referred to management. Only authorised persons may disclose information classified above Public, and then only to persons whose identity and validity to receive such information has been confirmed."

EXPLANATORY NOTES

Great care is to be exercised when answering the telephone and giving out information of any kind over this medium. With Caller Line Identifier (CLI) it is possible to identify the caller before answering, and to treat the call accordingly. Your *PBX* will record the CLI details where available and block any suspect numbers. See *Speaking to Customers* and *Speaking to the Media*.

Information Security issues to be considered when implementing your policy include the following:

- Inadvertently revealing sensitive information to the press.
- The inadvertent exposure of confidential information by staff talking to a caller.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.3 Confidentiality agreements

Policy 090314
Sharing Confidential Information with Family Members

SUGGESTED POLICY STATEMENT

"All data and information not in the public domain, relating to the organisation's business and its employees, must remain confidential at all times."

EXPLANATORY NOTES

Confidential information is classified into various levels of sensitivity and as such, must not be divulged to family members who do not have clearance to receive such information. See also *Classifying Information*.

Information Security issues to be considered when implementing your policy include the following:

- Confidential information may be leaked inadvertently via a 'trusted' family member.
- Confidential data given to unauthorised people by a family member with a possible grudge.
- Organisation information on laptops or documents brought home may be destroyed in error.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.3 Confidentiality agreements

Policy 090315
Gossiping and Disclosing Information

SUGGESTED POLICY STATEMENT

"All data and information not in the public domain, relating to the organisation's business and its employees, must remain confidential at all times."

EXPLANATORY NOTES

Office gossip is often considered harmless, however if it includes sensitive information then a casual chat round the coffee machine is not the appropriate forum. To an eavesdropper intent on getting confidential information, gossip is a good source of information. Careless discussion of organisation matters must be considered a security breach.

Information Security issues to be considered when implementing your policy include the following:

- The organisation's information may be disclosed in gossip and then used by ill intentioned persons.
- Inappropriate actions could be taken as the result of gossiping.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.3 Confidentiality agreements

Policy 090316
Spreading Information through the Office 'Grape Vine'

SUGGESTED POLICY STATEMENT

"All data and information not in the public domain, relating to the organisation's business and its employees, must remain confidential at all times."

EXPLANATORY NOTES

The free flow of relevant information within an organisation contributes to staff being a happy and productive team, and it eliminates any need for an 'office grape vine', which is notorious for passing on unverified information. Additionally, it may enable hackers to gain entry to your data.

Information Security issues to be considered when implementing your policy include the following:

- Organisation information is passed to unauthorised parties over the grape vine.
- Inappropriate actions could be taken as the result of gossiping.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.3 Confidentiality agreements

Policy 090317
Playing Games on Office Computers

SUGGESTED POLICY STATEMENT

"The playing of games on office PCs or laptops is prohibited."

EXPLANATORY NOTES

Additionally to the obvious issues of time wasted in playing games, there are those of the use of unauthorised software and potential virus risks. Such activities should not be permitted on organisation equipment and systems.

Information Security issues to be considered when implementing your policy include the following:

- Organisation systems may be attacked by malicious software introduced from a PC game program.
- A wastage of the organisation's resources and a possible breach of trust between employer and employee. Playing games is unlikely to be an effective use of one's time and can lead to disciplinary action.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.5 Prevention of misuse of information processing facilities

Policy 090318
Using Office Computers for Personal Use

SUGGESTED POLICY STATEMENT

"Using the organisation's computers for personal / private business is strongly discouraged."

EXPLANATORY NOTES

The use of office computers for personal use should not be permitted unless specific authorisation is granted by management.

Information Security issues to be considered when implementing your policy include the following:

- The organisation's systems can be attacked by malicious software introduced via a personal data disc being used on the network for non-organisation work.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.5 Prevention of misuse of information processing facilities

Sub-Chapter 04
HR Management

Policy 090401 **Dealing with Disaffected Staff**

Policy 090402 **Taking Official Notes of Employee Meetings**

Policy 090401
Dealing with Disaffected Staff

SUGGESTED POLICY STATEMENT

"Management must respond quickly yet discreetly to indications of staff disaffection, liaising as necessary with Human Resources management and the Information Security Officer."

EXPLANATORY NOTES

Disaffected staff can present a significant risk as they are still deemed trusted employees, but their potential to inflict damage is high. All staff will usually become aware of what *Information Assets* are of value to the organisation and, although they may not have direct access themselves, they may be able to obtain access through personal relationships.

Information Security issues to be considered when implementing your policy include the following:

- Staff whose personal circumstances have changed (e.g. financial) or who have a grievance may begin to act differently. Their change in behaviour could alert you to the possibility of a breach (or attempted breach) of your Information Security.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3 (Objective) Responding to security incidents and malfunctions

Policy 090402
Taking Official Notes of Employee Meetings

SUGGESTED POLICY STATEMENT

"Employee meeting and interview records must be formally recorded, with the contents classified as Highly Confidential and made available only to authorised persons."

EXPLANATORY NOTES

Interviews held with employees are to be formally recorded and the minutes agreed. These documents are to be treated with the same level of confidentiality as the meeting itself.

Information Security issues to be considered when implementing your policy include the following:

- Where employee interview information is not kept confidential, the organisation risks both contravention of legal requirements and staff grievance.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.4 Data protection and privacy of personal information

Sub-Chapter 05
Staff Leaving Employment

Policy 090501 **Handling Staff Resignations**

Policy 090502 **Completing Procedures for Staff Leaving Employment**

Policy 090503 **Obligations of Staff Transferring to Competitors**

Policy 090501
Handling Staff Resignations

SUGGESTED POLICY STATEMENT

"Upon notification of staff resignations, Human Resources management must consider with the appointed Information Security Officer whether the member of staff's continued system access rights constitutes an unacceptable risk to the organisation and, if so, revoke all access rights."

EXPLANATORY NOTES

Staff resignations occur from time to time and in the main are harmonious. However, whenever a member of staff resigns, there is the possibility that the person may be resentful of some issue, and could subsequently potentially act in a manner which could jeopardise the security of the organisation.

Information Security issues to be considered when implementing your policy include the following:

- Staff resignations can be followed by a loss of loyalty, especially where the individual involved perceives that their resignation has had little or no 'impact'. Such staff may become disgruntled and use their authority and / or systems *privileges* to 'sabotage' or 'mess up' information on the system.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3 (Objective) Responding to security incidents and malfunctions
9.2.1 User registration
9.2.2 Privilege management
9.2.4 Review of user access rights

Policy 090502
Completing Procedures for Staff Leaving Employment

SUGGESTED POLICY STATEMENT

"Departing staff are to be treated sensitively, particularly with regard to the termination of their access privileges."

EXPLANATORY NOTES

Staff who resign should be treated sensitively or they may become disgruntled and / or simply leave without adequate 'hand over' to colleagues etc.

Information Security issues to be considered when implementing your policy include the following:

- Some staff who resign may decide, or be obliged, to depart immediately, be it for personal reasons or due to the sensitivity of their position. Unless the organisation has procedures for handling this situation, it may suffer loss or damage to its information as a form of retribution or for personal gain.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.2.4 Review of user access rights

Policy 090503
Obligations of Staff Transferring to Competitors

SUGGESTED POLICY STATEMENT

"System and information access rights of employees who are transferring to competitors must be terminated immediately."

EXPLANATORY NOTES

Depending upon the terms and conditions of employment, staff may be contractually precluded from working for a competitor for a set number of years following resignation, retirement or termination. In practice, however, this may not deter such staff. They may be prepared to risk the potential consequences for the sake of perceived immediate gain. Thus, even though an organisation may possibly have the opportunity for legal redress, the damage may already have been done. This is a difficult legal area and legal advice should always be sought.

Information Security issues to be considered when implementing your policy include the following:

- Where your former employee disregards your Non Disclosure Agreement, valuable information may be revealed, thus potentially damaging your competitive position. See *Non Disclosure Agreements*.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.2.4 Review of user access rights

Sub-Chapter 06
HR Issues Other

Policy 090601 Recommending Professional Advisors

Policy 090601
Recommending Professional Advisors

SUGGESTED POLICY STATEMENT

"The organisation does not encourage the recommending of professional advisors. References may however be given by authorised members of staff."

EXPLANATORY NOTES

When asked to recommend a professional advisor you must make sure that their credentials will stand scrutiny. Your own credibility is used as a guide as to the validity of any claims made by your recommended advisor. Recommendations are to be discouraged to avoid potential liability for poor quality advice or service.

Information Security issues to be considered when implementing your policy include the following:

- Where a recommendation is made, the association with your organisation may lead to loss of credibility in general and possible legal liability.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.1.3 Confidentiality agreements

CHAPTER 10
CONTROLLING E-COMMERCE INFORMATION SECURITY

Sub-Chapter 01 E-Commerce Issues

Sub-Chapter 01
E-Commerce Issues

Policy 100101	**Structuring E-Commerce Systems including Web Sites**
Policy 100102	**Securing E-Commerce Networks**
Policy 100103	**Configuring E-Commerce Web Sites**
Policy 100104	**Using External Service Providers for E-Commerce**

Policy 100101
Structuring E-Commerce Systems including Web Sites

SUGGESTED POLICY STATEMENT

" e-commerce processing systems including the e-commerce Web site(s) are to be designed with protection from malicious attack given the highest priority."

EXPLANATORY NOTES

The fundamental rule for keeping an e-commerce Web site secure is that your entire e-commerce system must be protected with consistent and appropriate security measures. It is not enough to simply safeguard the interaction between the customer and the Web site's server.

The software components that comprise an organisation's e-commerce Web site are not secure 'out of the box', because the individual components are complex and often not designed with security in mind. Therefore it is important to analyse each component for its security weaknesses and protect it accordingly.

You may find this diagram helpful which gives an overview of the main components in your e-commerce planning.

Information Security issues to be considered when implementing your policy include the following:

- e-Commerce Web sites can fail through a lack of adequate technical planning. This can damage your business, irretrievably because of the wide public exposure on the Internet.

Caution : e-Commerce is, by definition, 'hi-tech', and you will require input and guidance from specialists in the field. The risks of not involving specialists can be great.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.3 Electronic commerce security
9.4 Network Access control
10.1.1 Security requirements analysis and specifications

Policy 100102
Securing E-Commerce Networks

SUGGESTED POLICY STATEMENT

"e-commerce related Web site(s) and their associated systems are to be secured using a combination of technology to prevent and detect intrusion together with robust procedures using dual control, where manual interaction is required."

EXPLANATORY NOTES

E-Commerce operates on and through communications networks, principally the Internet. Therefore, safeguarding the integrity of your Web site and its associated software and data is critical, especially where *24x7* operation is expected.

Information Security issues to be considered when implementing your policy include the following:

- Malicious or opportunistic damage may occur if your network safeguards fail to prevent unauthorised access to your corporate network, when you open it up for Web based e-commerce.
- If the network access controls to your Web server are poor, your site may be subject to unauthorised access ('hacked'), leading to theft (e.g. of credit card numbers) or corruption of data.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.3 Electronic commerce security
9.1.1 Access control policy
9.4 Network Access control
9.7.2 Network Monitoring system use

Policy 100103
Configuring E-Commerce Web Sites

SUGGESTED POLICY STATEMENT

"The organisation's e-commerce Web site(s) must be configured carefully by specialist technicians to ensure that the risk from malicious intrusion is not only minimised but that any data captured on the site, is further secured against unauthorised access using a combination of robust access controls and encryption of data."

EXPLANATORY NOTES

Whilst the individual technologies to set up and maintain a Web site are quite mature, there are many pitfalls for the unwary. Expert guidance is essential if your e-commerce Web site is to withstand attack.

Information Security issues to be considered when implementing your policy include the following:

- You may set an inappropriate level of *privilege* by accepting the *default* values when configuring your Web site. This could give 'carte-blanche' access to the files on your Web server when the Web software is run.

e.g. The System Administrator sets up a Web site and needs to set up the server - logically using the most powerful '*super user*' *privilege*. Without any real concern for the ongoing Information Security implications, the privilege is left at 'super user' and results in **all** software being run at this level. Anyone compromising the security of the Web server would then gain access at this level and would be able to read, write, create, or execute any file on this server.

- E-commerce transactions will always require user input, execution and update. This is often accomplished on a Web server using a *Common Gateway Interface* - CGI script. However, such scripts can be exploited by malicious users to execute system commands for illegal purposes.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.3 Electronic commerce security

Policy 100104
Using External Service Providers for E-Commerce

SUGGESTED POLICY STATEMENT

"Where third parties are involved in e-commerce systems and delivery channels, it is essential that they are able to meet the resilience and Information Security objectives of the organisation."

EXPLANATORY NOTES

The technical operation of your Web site may be managed by an Internet Service Provider (ISP), on whose reliability of service your organisation is entirely dependent. This topic considers ISP selection, secure payment systems and, briefly, aspects of contract law.

Information Security issues to be considered when implementing your policy include the following:

- Concerns over the security features of your e-commerce payment system may circulate. As a result, your organisation's reputation may be damaged, leading to revenue being lost and trading partners withdrawing.
- Reliability problems with your Web site, compounded by omissions in the *Service Level Agreement* (SLA) with your ISP, may jeopardise your commercial activities, damaging both your cash flow and, additionally, your reputation.
- If e-mails that contain details about e-commerce transactions are accidentally deleted, it could be detrimental to any subsequent legal proceedings.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.7.3	Electronic commerce security
4.2.2	Security requirements in third party contracts
4.3.1	Security requirements in outsourcing contracts
10.5.5	Outsourced software development

CHAPTER 11
DELIVERING TRAINING AND STAFF AWARENESS

Sub-Chapter 01 Awareness

Sub-Chapter 02 Training

Sub-Chapter 01
Awareness

Policy 110101	**Delivering Awareness Programmes to Permanent Staff**
Policy 110102	**Third Party Contractor : Awareness Programmes**
Policy 110103	**Delivering Awareness Programmes to Temporary Staff**
Policy 110104	**Drafting Top Management Security Communications to Staff**
Policy 110105	**Providing Regular Information Updates to Staff**

Policy 110101
Delivering Awareness Programmes to Permanent Staff

SUGGESTED POLICY STATEMENT

"Permanent staff are to be provided with Information Security awareness tools to enhance awareness and educate them regarding the range of threats and the appropriate safeguards."

EXPLANATORY NOTES

It only takes a single lapse to put your organisation's data and information resources at risk. Therefore, ideally, staff would develop their awareness of Information Security risks so that it almost becomes second nature.

Information Security issues to be considered when implementing your policy include the following:

- Sensitive data may be acquired unlawfully, damaged, or modified because staff have become complacent.
- Sensitive data may be compromised by staff assuming new duties without specific Information Security training.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.2.1 Information security education and training

Policy 110102
Third Party Contractor : Awareness Programmes

SUGGESTED POLICY STATEMENT

"An appropriate summary of the Information Security Policies must be formally delivered to any such contractor, prior to any supply of services."

EXPLANATORY NOTES

Third party contractors coming into the organisation are usually specialists or professionals, and it is easy to assume that their expertise also extends to Information Security. In fact, the converse is true: they are least likely to appreciate your organisational Information Security arrangements. Permanent staff should be aware of the risks posed by such third party contractors on their site.

Information Security issues to be considered when implementing your policy include the following:

- Data may be lost in error or through negligence by contractor staff inadequately trained in Information Security.
- Data may be lost because technical data security measures are installed incorrectly by contractors, and their alarms and messages are misinterpreted.
- Information Security breaches may occur, and information be compromised, because contractor staff are unaware of the scope of the organisation's Information Security safeguards.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.2.2 Security requirements in third party contracts
6.2.1 Information security education and training

Policy 110103
Delivering Awareness Programmes to Temporary Staff

SUGGESTED POLICY STATEMENT

"An appropriate summary of the Information Security Policies must be formally delivered to, and accepted by, all temporary staff, prior to their starting any work for the organisation."

EXPLANATORY NOTES

Temporary staff members are viewed as a transient resource that is used to maximise productivity and minimise costs. Although they have access to company information, they are not usually held accountable for their actions, as they are 'not part of the company'. This increases the risk of Information Security breaches.

Information Security issues to be considered when implementing your policy include the following:

- Loss of data may be caused by errors and negligence of temporary staff, unaware of Information Security issues.
- Information Security breaches may occur, and information be compromised, because temporary staff are unaware of the scope of the organisation's Information Security safeguards.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.2.1 Information security education and training

Policy 110104
Drafting Top Management Security Communications to Staff

SUGGESTED POLICY STATEMENT

"The senior management of the organisation will lead by example by ensuring that Information Security is given a high priority in all current and future business activities and initiatives."

EXPLANATORY NOTES

The need for top level management to take the lead in Information Security awareness initiatives, and to cascade them down the organisation.

Information Security issues to be considered when implementing your policy include the following:

- Sensitive data can be acquired unlawfully or modified if senior management becomes complacent about Information Security.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.2 Information security co-ordination

Policy 110105
Providing Regular Information Updates to Staff

SUGGESTED POLICY STATEMENT

"The organisation is committed to providing regular and relevant Information Security awareness communications to all staff by various means, such as electronic updates, briefings, newsletters, etc."

EXPLANATORY NOTES

Staff awareness of Information Security issues can fade, unless it is continually reinforced. Conversely, staff have a valuable role to play in giving feedback on the effectiveness of the organisation's Information Security measures.

Information Security issues to be considered when implementing your policy include the following:

- Staff awareness of Information Security issues can fade unless it is continually reinforced. Such lack of attention may expose sensitive data to outsiders. Valuable feedback from staff may not be encouraged.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.1.2 Information security co-ordination

Sub-Chapter 02
Training

Policy 110201 Information Security Training on New Systems

Policy 110202 Information Security Officer : Training

Policy 110203 User : Information Security Training

Policy 110204 Technical Staff : Information Security Training

Policy 110205 Training New Recruits in Information Security

Policy 110201
Information Security Training on New Systems

SUGGESTED POLICY STATEMENT

"The organisation is committed to providing training to all users of new systems to ensure that their use is both efficient and does not compromise Information Security."

EXPLANATORY NOTES

You should be able to implement new systems without this resulting in concerns over Information Security, a downgrading of your existing Information Security framework, or security breaches.

Information Security issues to be considered when implementing your policy include the following:

- Confidential data may be lost, damaged or compromised by staff who are unfamiliar with the new systems.
- Data may be lost because the new Information Security systems are installed incorrectly, and their alarms and messages are misinterpreted.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.2.1 Information security education and training

Policy 110202
Information Security Officer : Training

SUGGESTED POLICY STATEMENT

"Periodic training for the Information Security Officer is to be prioritised to educate and train in the latest threats and Information Security techniques."

EXPLANATORY NOTES

The Information Security Officer oversees the operation of your organisation's Information Security measures. This includes monitoring all company Information Security measures and systems, and safeguarding all company information. Anyone in this position needs a high level of skill and knowledge in Information Security matters. Ongoing training both in generic Information Security technology and in particular issues, such as intrusion counter measures, will enhance your company's Information Security profile.

Information Security issues to be considered when implementing your policy include the following:

- The organisation's Information Security measures can be compromised by new malicious software or techniques unknown to your Information Security team.
- Confidential data may be lost or compromised because the Information Security team implements inappropriate measures.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.2.1 Information security education and training

Policy 110203
User : Information Security Training

SUGGESTED POLICY STATEMENT

" Individual training in Information Security is mandatory, with any technical training being appropriate to the responsibilities of the user's job function. Where staff change jobs, their Information Security needs must be re-assessed and any new training provided as a priority."

EXPLANATORY NOTES

The level of Information Security training required for individual system users must be appropriate to their specific duties, so that the confidentiality, integrity, and availability of information they would normally handle is safeguarded.

Information Security issues to be considered when implementing your policy include the following:

- Confidential information may be damaged, lost or compromised because staff are unaware of the Information Security issues.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.2.1 Information security education and training

Policy 110204
Technical Staff : Information Security Training

SUGGESTED POLICY STATEMENT

"Training in Information Security threats and safeguards is mandatory, with the extent of technical training to reflect the job holder's individual responsibility for configuring and maintaining Information Security safeguards. Where IT staff change jobs, their Information Security needs must be re-assessed and any new training provided as a priority."

EXPLANATORY NOTES

By virtue of their position, technical staff both protect the organisation's information, but equally, may inadvertently (or maliciously) put it at greater risk. Therefore it is essential that they be trained to a level of competence in Information Security that matches their duties and responsibilities.

Information Security issues to be considered when implementing your policy include the following:

- Where technical staff are poorly trained, their lack of knowledge risks the organisation's computer operations and information systems. The damage can be substantial.
- Where technical security components have been installed incorrectly, data may be lost or damaged with any alarms or alert messages possibly being misinterpreted.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.2.1 Information security education and training

Policy 110205
Training New Recruits in Information Security

SUGGESTED POLICY STATEMENT

"All new staff are to receive mandatory Information Security awareness training as part of induction."

EXPLANATORY NOTES

All management and staff are responsible for Information Security, including those new to the organisation. It is vital they are brought 'up to speed' quickly to avoid unnecessary Information Security breaches.

Information Security issues to be considered when implementing your policy include the following:

- Confidential data may be lost, damaged or compromised by staff with insufficient training.
- Data may be lost in error or through negligence because staff have poor Information Security training.
- Data may be lost because Information Security measures have been installed incorrectly and their alarms and messages are misinterpreted.
- Confidential information may be compromised if new staff are not aware of the scope of the organisation's Information Security measures.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.2.1 Information security education and training

CHAPTER 12
DEALING WITH PREMISES RELATED CONSIDERATIONS

Sub-Chapter 01
Premises Security

Policy 120101	**Preparing Premises to Site Computers**
Policy 120102	**Securing Physical Protection of Computer Premises**
Policy 120103	**Ensuring Suitable Environmental Conditions**
Policy 120104	**Physical Access Control to Secure Areas**
Policy 120105	**Challenging Strangers on the Premises**

Policy 120101
Preparing Premises to Site Computers

SUGGESTED POLICY STATEMENT

"The sites chosen to locate computers and to store data must be suitably protected from physical intrusion, theft, fire, flood and other hazards."

EXPLANATORY NOTES

In the context of Information Security, the term 'premises' refers to any area in which hardware is located; it may range from a corner in an office to an entire building. It is important to consider the choice of premises for your computer hardware carefully because it is difficult to make changes once a location has been selected.

The size of the area will be dictated by the amount of hardware to be housed. The environmental requirements for the selected area will be specified by the manufacturer of your hardware. The physical security measures adopted, however, are likely to depend on the value of the hardware, the sensitivity of your data and the required level of service *resilience*.

Information Security issues to be considered when implementing your policy include the following:

- Malicious damage is likely to threaten your ability to meet your business requirements and will result in unnecessary expenditure.
- The non-availability of essential services is likely to threaten your normal operations.
- Accidental damage to premises may threaten normal business operations.
- The theft of equipment would not only cause unnecessary expenditure, but may also disrupt the operation of critical systems.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.1 Equipment siting and protection

Policy 120102
Securing Physical Protection of Computer Premises

SUGGESTED POLICY STATEMENT

"Computer premises must be safeguarded against unlawful and unauthorised physical intrusion."

EXPLANATORY NOTES

The physical dangers that threaten your computer premises and the means by which they may be lessened or eliminated.

Information Security issues to be considered when implementing your policy include the following:

- Unlawful access may be gained with a view to theft, damage, or other disruption of operations.
- Unauthorised and illegal access may take place covertly to steal, damage, or otherwise disrupt operations.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.1.1 Physical security perimeter

Policy 120103
Ensuring Suitable Environmental Conditions

SUGGESTED POLICY STATEMENT

"When locating computers and other hardware, suitable precautions are to be taken to guard against the environmental threats of fire, flood and excessive ambient temperature / humidity."

EXPLANATORY NOTES

The environmental dangers that threaten your computer premises, and the means by which they may be lessened or eliminated.

Information Security issues to be considered when implementing your policy include the following:

- Serious fire damage could make it impossible to continue business operations.
- Flooding can make it impossible to continue business in any form with severe implications.
- Failure of the air conditioning unit(s) can unsettle business operations (especially in large computer rooms) and potentially result in stoppage.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.1.3 Securing offices, rooms and facilities

Policy 120104
Physical Access Control to Secure Areas

SUGGESTED POLICY STATEMENT

"All computer premises must be protected from unauthorised access using an appropriate balance between simple ID cards to more complex technologies to identify, authenticate and monitor all access attempts."

EXPLANATORY NOTES

Because of the dangers of theft, vandalism and unauthorised use of your systems, you should consider restricting the number of people who have physical access to the area in which your computers are housed. This requirement should be taken into account when premises are being chosen. See *Preparing Premises to Site Computers*.

Any access control system is likely to have to handle the following categories of personnel, each of whom will have different access conditions:

1) Operators and, sometimes, system users who regularly work within the secure area,
2) Engineers and other support staff who require periodic access,
3) Others, who require access only rarely.

Information Security issues to be considered when implementing your policy include the following:

- Unauthorised staff may gain access to restricted areas, and damage or disruption results.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.1.2 Physical entry controls

Policy 120105
Challenging Strangers on the Premises

SUGGESTED POLICY STATEMENT

"All employees are to be aware of the need to challenge strangers on the organisation's premises."

EXPLANATORY NOTES

In small organisations people know one another, and any unusual activities or strangers will be noticed very quickly. In large organisations this is less likely. Any apparent strangers may turn out to be a new staff member or just someone whom you have not seen before. That notwithstanding, do not be afraid to challenge strangers, as they may just as easily be an unauthorised person intending to compromise your organisation.

Information Security issues to be considered when implementing your policy include the following:

- Unescorted visitors /strangers may access confidential material or damage/remove organisation property.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.1.3 Securing offices, rooms and facilities

Sub-Chapter 02
Data Stores

Policy 120201 Managing On-Site Data Stores

Policy 120202 Managing Remote Data Stores

Policy 120201
Managing On-Site Data Stores

SUGGESTED POLICY STATEMENT

"On-site locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level."

EXPLANATORY NOTES

Data stores hold your removable media. They form a vital link in your *Backup and Recovery* procedures, since they should contain duplicate copies of your essential data. Usually 'on-site' data stores are maintained in conjunction with a 'remote data store' located far enough away from your main computer site, not to be affected by any disaster that may befall it. This section is primarily concerned with 'on-site' data stores. Clearly, losing your stored data could have very serious repercussions.

Information Security issues to be considered when implementing your policy include the following:

- Theft / Fraud of media, or malicious damage, would threaten the confidentiality of your data, and may make it difficult or impossible for *Systems Operations* to perform their duties.
- Accidental damage may render it difficult or impossible to process or restore information, causing possible loss to your organisation.
- Loss of media and data may seriously compromise the ability of Systems Operations to maintain an efficient system.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.1.2 Physical entry controls
7.1.3 Securing offices, rooms and facilities

Policy 120202
Managing Remote Data Stores

SUGGESTED POLICY STATEMENT

"Remote locations where data is stored must provide access controls and protection which reduce the risk of loss or damage to an acceptable level."

EXPLANATORY NOTES

Remote Data Stores are located at a distance from your main processing site. The distance should be adequate to ensure that a major disaster, such as a fire or explosion at your main site, will not affect the Remote Data Store. Sufficient data should be stored there to allow restoration, if your primary data is destroyed.

Remote data stores face the same threats as on-site data stores, but there are some additional threats which are particular to them.

Information Security issues to be considered when implementing your policy include the following:

- Theft of data may render it difficult or impossible to meet your business requirements, or may be used fraudulently against your organisation.
- Accidental damage may render it difficult or impossible to meet your business requirements.
- Loss and malicious damage may render it difficult or impossible to meet your business requirements.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.1.1 Physical security perimeter
7.1.2 Physical entry controls
7.1.3 Security offices, rooms and facilities

Sub-Chapter 03
Other Premises Issues

Policy 120301 **Electronic Eavesdropping**

Policy 120302 **Cabling Security**

Policy 120303 **Disaster Recovery Plan**

Policy 120301
Electronic Eavesdropping

SUGGESTED POLICY STATEMENT

" Electronic eavesdropping should be guarded against by using suitable detection mechanisms, which are to be deployed if and when justified by the periodic risk assessments of the organisation."

EXPLANATORY NOTES

'Electronic eavesdropping' is the term applied to monitoring electronic radiation from computer equipment and reconstituting it into discernible information. Although this sounds like a highly technical process, sometimes it can be undertaken easily with inexpensive equipment. The method can be applied to most computer equipment, but it is particularly effective with conventional (*CRT*-based) VDUs, situated in solitary locations close to the outer wall of your building. Although electronic eavesdropping is a relatively obscure threat to the confidentiality of your data, it is wise to take the possibility of it into account when selecting the location of computer screens.

Information Security issues to be considered when implementing your policy include the following:

- Loss of Confidentiality because information is 'stolen' from your screen.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

Introduction	How to establish security requirements Assessing security risks
7.2.1	Equipment siting and protection

Policy 120302
Cabling Security

SUGGESTED POLICY STATEMENT

"The security of network cabling must be reviewed during any upgrades or changes to hardware or premises."

EXPLANATORY NOTES

The security of your cabling should be considered both when your computer premises are set up initially, and, subsequently, when hardware enhancements are carried out. See also *Installing and Maintaining Network Cabling*.

Information Security issues to be considered when implementing your policy include the following:

- Cables may be damaged with a resultant reduction in reliability and / or the loss of your network.
- Any intrusion into your network may threaten your information systems and hence the confidentiality of your information.
- A failure to observe Health and Safety regulations may threaten the well-being of staff and render you liable to prosecution.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

7.2.3 Cabling security

Policy 120303
Disaster Recovery Plan

SUGGESTED POLICY STATEMENT

"Owners of the organisation's information systems must ensure that disaster recovery plans for their systems are developed, tested, and implemented."

EXPLANATORY NOTES

The configuration of your business premises and particularly the location of your hardware affect your *Disaster Recovery Plan* (DRP). This should allow for access to any hardware which remains undamaged by disaster.

Information Security issues to be considered when implementing your policy include the following:

- Lack of continuity of service would likely render it difficult or impossible to meet your business requirements.
- A Disaster Recovery Plan is an important preliminary part of the organisation's Business Continuity Plan (BCP). A severe incident can affect any organisation at any time and all organisations should ensure that they have both a DRP and a BCP.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

11.1.1 Business continuity management process

CHAPTER 13
DETECTING AND RESPONDING TO IS INCIDENTS

Sub-Chapter 01
Reporting Information Security Incidents

Policy 130101
Reporting Information Security Incidents

SUGGESTED POLICY STATEMENT

"All suspected Information Security incidents must be reported promptly to the appointed Information Security Officer."

EXPLANATORY NOTES

An Information Security incident can be defined as any occurrence which in itself does not necessarily compromise Information Security, but which could result in it being compromised. An example is a multiple login failure on a single user account, leading to that account being locked out. This topic discusses reporting structures for Information Security incidents.

Information Security issues to be considered when implementing your policy include the following:

- A member of staff may not report an Information Security incident because there are no procedures in place to do so, resulting in a chain of events that leads to your organisation's information systems being compromised.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3.1 Reporting security incidents

Policy 130102
Reporting IS Incidents to Outside Authorities

SUGGESTED POLICY STATEMENT

"Information Security incidents must be reported to outside authorities whenever this is required to comply with legal requirements or regulations. This may only be done by authorised persons."

EXPLANATORY NOTES

You may be obliged to report certain Information Security incidents to external authorities, such as: regulatory bodies for your industry, third party associates (for example your ISP) and law enforcement agencies. The responsibility for making such reports usually lies with senior management.

Information Security issues to be considered when implementing your policy include the following:

- Your organisation may unwittingly be aiding or abetting an offence by not reporting an Information Security incident to outside authorities. Future investigations could lead to your organisation as being the source of the offence.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3.1 Reporting security incidents

Policy 130103
Reporting Information Security Breaches

SUGGESTED POLICY STATEMENT

"Any Information Security breaches must be reported without any delay to the appointed Information Security Officer to speed the identification of any damage caused, any restoration and repair and to facilitate the gathering of any associated evidence."

EXPLANATORY NOTES

An Information Security breach can be regarded as a series of Information Security incidents whose ultimate result is damage to or loss of data from an information system. The breach could be physical (e.g. a break-in and subsequent theft) or 'procedural' (e.g. unauthorised computer access, resulting in loss of data). This topic discusses reporting structures to deal with Information Security breaches.

Information Security issues to be considered when implementing your policy include the following:

- A lack of formal reporting procedure for Information Security breaches may delay resumption of business operations.
- Delays in commencing investigations by the Information Security Officer can greatly increase the potential losses associated with the reported breach.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3.1 Reporting security incidents

Policy 130104
Notifying Information Security Weaknesses

SUGGESTED POLICY STATEMENT

"All identified or suspected Information Security weaknesses are to be notified immediately to the Information Security Officer."

EXPLANATORY NOTES

Information Security weaknesses can manifest themselves in the area of software and physical access to restricted areas. For details of physical access weaknesses refer to *Dealing with Premises Related Considerations*.

Information Security issues to be considered when implementing your policy include the following:

- Where there is no procedure to report Information Security weaknesses, there is a possibility that inexperienced staff may try to correct an Information Security weakness in an application program or an operating system and interrupt business critical processing.
- Where a risk assessment study has not been carried out it may be difficult to identify all areas of information security weakness.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3.2 Reporting security weaknesses

Policy 130105
Witnessing an Information Security Breach

SUGGESTED POLICY STATEMENT

"Persons witnessing Information Security incidents or breaches should report them to the Information Security Officer without delay."

EXPLANATORY NOTES

Awareness and vigilance to possible Information Security breaches is the best way to minimise the intended consequences of an actual Information Security breach. Users **must** be made aware that Information Security is everybody's responsibility. This must be ingrained into your organisation's culture by awareness sessions, training, and online Information Security intelligence data. This topic looks at the consequences of not reporting an Information Security breach, which you witness.

Information Security issues to be considered when implementing your policy include the following:

- By not reporting a potential Information Security breach, a member of staff may be implicated in further investigations, which may lead to your organisation being prosecuted.
- If staff are not aware of the importance of reporting potential information security breaches, then incidents can remain uninvestigated for unacceptable periods.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3.1 Reporting security incidents

Policy 130106
Being Alert for Fraudulent Activities

SUGGESTED POLICY STATEMENT

"Employees are expected to remain vigilant for possible fraudulent activities."

EXPLANATORY NOTES

Complacency in your organisation over Information Security matters can lead to fraudulent activities going unnoticed. For organisation staff to be aware of such risks, they need to be given pertinent information on a regular basis. This topic looks at ways you can achieve a high level of awareness.

Information Security issues to be considered when implementing your policy include the following:

- A lack of commitment to your Information Security Policies by staff may result in fraudulent activities going unnoticed, resulting in financial loss and / or damage to your organisation's reputation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.2.1 Information security education and training

Sub-Chapter 02
Investigating Information Security Incidents

Policy 130201 Investigating the Cause and Impact of IS Incidents

SUGGESTED POLICY STATEMENT

"Information Security incidents must be properly investigated by suitably trained and qualified personnel."

EXPLANATORY NOTES

Your investigation into an Information Security incident must identify its cause and appraise its impact on your systems or data. This will assist you in planning how to prevent a reoccurrence.

Information Security issues to be considered when implementing your policy include the following:

- A recurrence of data loss / corruption during a particular phase of processing may be indicative of the inappropriate closure of a prior Information Security incident.
- If the organisation entrusts its information security to untrained and inexperienced personnel it may incur the risks involved in adequate responses to reported incidents. Suitable training should always be provided.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3 Responding to security incidents and malfunctions

Policy 130202
Collecting Evidence of an Information Security Breach

SUGGESTED POLICY STATEMENT

"Evidence relating to an Information Security breach must be properly collected and forwarded to the Information Security Officer."

EXPLANATORY NOTES

Evidence of an Information Security breach must be collected to comply with statutory, regulatory or contractual obligations and avoid breaches of criminal or civil law. Advice on specific legal requirements should be sought from the organisation's legal advisers. Legal requirements vary from country to country.

Information Security issues to be considered when implementing your policy include the following:

- Evidence collected for a disciplinary hearing may be too weak to bring disciplinary charges. The threat to security posed by the staff member remains.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

12.1.7 Collection of evidence

Policy 130203
Recording Information Security Breaches

SUGGESTED POLICY STATEMENT

"Evidence relating to a suspected Information Security breach must be formerly recorded and processed."

EXPLANATORY NOTES

The practice of recording all aspects of Information Security breaches helps organisations develop preventative measures which minimise the likelihood of a reoccurrence. Such reports must contain a full account of actions undertaken by staff (and any third parties) who contained the breach. They are also a useful source of feedback for Information Security policies.

Information Security issues to be considered when implementing your policy include the following:

- The lack of a record of the steps taken to contain an Information Security breach may mean that your organisation loses valuable information, which could help to prevent future breaches of Information Security.
- Inadequate procedures for dealing with Information Security breaches may significantly increase potential losses associated with that breach.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3.1 Reporting security incidents

Policy 130204
Responding to Information Security Incidents

SUGGESTED POLICY STATEMENT

"The Information Security Officer must respond rapidly but calmly to all Information Security incidents, liaising and coordinating with colleagues to both gather information and offer advice."

EXPLANATORY NOTES

All Information Security incidents have to be evaluated according to their particular circumstances, and this may, or may not, require various departments to be involved: Technical, Human Resources, Legal and the owners of information (local department heads). If it appears that disciplinary action against a member of staff is required, this must be handled with tact.

Information Security issues to be considered when implementing your policy include the following:

- An inappropriate response to an Information Security incident may result in your organisation being subjected to further incidents, culminating in the loss of business critical services.
- Responses to Information Security incidents should be carried out in accordance with a predefined plan and procedure. If this process is not carefully followed there is the danger that the response will be haphazard and uncoordinated.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.1.3 Incident management procedures

Sub-Chapter 03
Corrective Activity

Policy 130301 Establishing Remedies to Information Security Breaches

Policy 130301
Establishing Remedies to Information Security Breaches

SUGGESTED POLICY STATEMENT

"A database of Information Security threats and 'remedies' should be created and maintained. The database should be studied regularly with the anecdotal evidence used to help reduce the risk and frequency of Information Security incidents in the organisation."

EXPLANATORY NOTES

The best way to stop Information Security breaches from reoccurring is to establish a database of past incidents and their solutions, and update it with reliable (internal and external) information about the latest threats. This topic suggests some sources of this type of information.

Information Security issues to be considered when implementing your policy include the following:

- An inappropriate remedy to resolve an Information Security breach may lead to excessive *downtime* of a business critical system.
- Information can be gathered from the Internet in respect of Information Security incidents occurring to organisations from all around the globe. Failure to keep abreast of recent developments in this field could result in time being wasted understanding the suspected incident.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

6.3.4 Learning from incidents

Sub-Chapter 04
Other Information Security Incident Issues

Policy 130401
Ensuring the Integrity of IS Incident Investigations

SUGGESTED POLICY STATEMENT

"The use of information systems must be monitored regularly with all unexpected events recorded and investigated. Such systems must also be periodically audited with the combined results and history strengthening the integrity of any subsequent investigations."

EXPLANATORY NOTES

The integrity and reliability of Security Incident investigations is greatly strengthened if your information systems are monitored and audited regularly.

Information Security issues to be considered when implementing your policy include the following:

- A data owner may inadvertently allow modifications of audit trails to be carried out by members of staff, thus hindering Information Security incident investigations.
- It is important that investigations into suspected Information Security incidents are formally recorded. This will ensure that the incident investigation may be audited at a later date.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

9.7.2 Monitoring system use
12.3.1 System audit controls
12.3.2 Protection of system audit tools

Policy 130402
Analysing IS Incidents Resulting from System Failures

SUGGESTED POLICY STATEMENT

"Information Security incidents arising from system failures are to be investigated by competent technicians."

EXPLANATORY NOTES

System failures may be the result of malicious activity, but differentiating these failures from hardware or known software bug failures requires experience and expertise.

Information Security issues to be considered when implementing your policy include the following:

- Incomplete analysis of a system failure may not reveal that the failure was due to malicious activity, thus leaving a back door opportunity for future disruption of services.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.1.3 Incident management procedures

Policy 130403
Breaching Confidentiality

SUGGESTED POLICY STATEMENT

"Breaches of confidentiality must be reported to the Information Security Officer as soon as possible."

EXPLANATORY NOTES

A breach of confidentiality is usually a disclosure of information. It must be considered as an Information Security incident and treated accordingly. This policy considers breaches of confidentiality arising from a breach of an employee's *Terms and Conditions* and from non compliance with a *Non Disclosure Agreement*.

Information Security issues to be considered when implementing your policy include the following:

- A third party contractor may leak confidential information about your organisation's product to a rival, causing you financial loss.
- An employee may disclose confidential information to a fellow employee, who then makes the information public, to the detriment of the organisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

4.2.2 Security requirements in third party contracts
6.1.3 Confidentiality agreements

Policy 130404
Establishing Dual Control / Segregation of Duties

SUGGESTED POLICY STATEMENT

" During the investigation of Information Security incidents, dual control and the segregation of duties are to be included in procedures to strengthen the integrity of information and data."

EXPLANATORY NOTES

Dual control and/or segregation of duties can be used to divide the responsibility of the completion of a process into separate, accountable actions, or to safeguard integrity (for example, of an Information Security investigation).

Information Security issues to be considered when implementing your policy include the following:

- An investigation into an Information Security incident may be compromised if a member of staff has access to an audit trail that recorded their actions during the incident.
- Whilst maintaining the required levels of confidentiality concerning potential incidents, at the appropriate time, the investigator should share his suspicions and findings with other responsible officers in affected departments to ensure that proper action can be taken.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.1.3 Incident management procedures
8.1.4 Segregation of duties

Policy 130405
Using Information Security Incident Check Lists

SUGGESTED POLICY STATEMENT

"Staff shall be supported by management in any reasonable request for assistance together with practical tools, such as security incident checklists, etc., in order to respond effectively to an Information Security incident."

EXPLANATORY NOTES

Information Security Incident Check Lists are used to verify the basic facts of security breaches and constitute part of the incident report. This topic looks at some of the features they can include.

Information Security issues to be considered when implementing your policy include the following:

- The lack of checklists at the outset of an Information Security investigation may delay implementing remedies, because establishing the basic circumstances of the incident takes an inordinate amount of time.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.1.3 Incident management procedures

Policy 130406
Detecting Electronic Eavesdropping and Espionage Activities

SUGGESTED POLICY STATEMENT

"Where a risk assessment has identified an abnormal high risk from the threat of electronic eavesdropping and / or espionage activities, all employees will be alerted and reminded of the specific threats and the specific safeguards to be employed."

EXPLANATORY NOTES

This topic discusses countermeasures available to protect against electronic eavesdropping and espionage techniques A wide variety of technology is available, so specialist advice may be needed to make the appropriate choice.

Information Security issues to be considered when implementing your policy include the following:

- A lack of knowledge about electronic espionage technology may result in highly confidential information about your organisation being disclosed.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

Introduction	How to establish security requirements Assessing security risks
6.2.1	Information Security education and training

Policy 130407
Monitoring Confidentiality of Information Security Incidents

SUGGESTED POLICY STATEMENT

"Information relating to Information Security incidents may only be released by authorised persons."

EXPLANATORY NOTES

Maintaining confidentiality of Information Security incidents whilst they are being investigated is important for the reputation of your organisation. This topic addresses some of the ways to protect confidentiality.

Information Security issues to be considered when implementing your policy include the following:

- Where unauthorised disclosure of an Information Security incident occurs, the conclusions drawn by those so informed, may result in serious damage to your organisation's reputation.
- Where it is legally required to notify the authorities of a suspected incident, this should only be done by an authorised official.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.1.3 Incident management procedures

CHAPTER 14
CLASSIFYING INFORMATION AND DATA

Sub-Chapter 01 Setting Classification Standards

Sub-Chapter 01
Setting Classification Standards

Policy 140101
Defining Information

SUGGESTED POLICY STATEMENT

"The organisation must record, maintain and update a data base of its information assets."

EXPLANATORY NOTES

Information can be defined as data which has meaning. It is the meaning of this data which has to be protected, in accordance with its worth to your organisation. This policy looks at ways to categorise your organisation's information.

Information Security issues to be considered when implementing your policy include the following:

- Confidential or important information held by your organisation could be lost or destroyed due to staff members treating information inappropriately, resulting in the loss of information which is critical to the business.
- If information is not classified to specify its level of sensitivity or confidentiality, then it is very difficult to protect sensitive documents or other information.
- If information ownership is not specified for each piece of data, document, spreadsheet or other information, then it is very difficult to manage and control access to that information.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.2.1 Classification guidelines

Policy 140102
Labelling Classified Information

SUGGESTED POLICY STATEMENT

"All information, data and documents are to be clearly labelled so that all users are aware of the ownership and classification of the information."

EXPLANATORY NOTES

Labelling of information makes decision making for your staff easier - they will immediately know how to handle the information they are dealing with, by reference to your organisation's published rules. This policy looks at various ways your organisation can label information.

Information Security issues to be considered when implementing your policy include the following:

- The incorrect labelling of information may lead to disclosure of that information into the public domain, resulting in loss of client confidence in your organisation.
- If an adequate labelling system is not properly designed and approved, consistency may not be applied by all users within the organisation.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.2.2 Information labelling and handling

Policy 140103
Storing and Handling Classified Information

SUGGESTED POLICY STATEMENT

"All information, data and documents must be processed and stored strictly in accordance with the classification levels assigned to that information."

EXPLANATORY NOTES

Storage and handling of information is important, because control over the state and location of the information maintains its integrity. This policy looks at some of the aspects of storage, and also considers how information changes over time.

Information Security issues to be considered when implementing your policy include the following:

- Highly confidential information, which has not been transported safely or destroyed securely, could be disclosed erroneously into the public domain, resulting in the loss of your organisation's reputation.
- Confidential information may retain its original classification when it should have been re-classified to a higher level of confidentiality. This could result in loss of the information due to its storage in an inappropriate location (physical or electronic).
- If a consistent system of information and document classification is not introduced, this could result in a lack of control, and misunderstanding over document access controls.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.6.3 Information handling procedures

Policy 140104
Isolating Top Secret Information

SUGGESTED POLICY STATEMENT

"All information, data or documents classified as highly sensitive (Top Secret) must be stored in a separate secure area."

EXPLANATORY NOTES

This policy considers information which can be considered as top secret - a classification level which exceeds the previously defined levels of highly confidential, confidential and sensitive. This type of information requires special storage and handling techniques.

Information Security issues to be considered when implementing your policy include the following:

- Information classified as 'Top Secret' held in your computer systems could be compromised and, in extremis, could result in the failure of your organisation's business.
- In order to protect high value information assets, secure areas containing top secret information are to be properly protected with additional levels of security.
- The access controls over secure areas containing top secret information are to be regularly reviewed and tested by qualified persons with appropriate security clearance.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.2.2 (b) Information labelling and handling
9.6.2 Sensitive system isolation

Policy 140105
Classifying Information

SUGGESTED POLICY STATEMENT

"All information, data and documents must be classified according to their level of confidentiality, sensitivity, value and criticality."

EXPLANATORY NOTES

Once information has been identified and the owner established, the next stage is to classify it according to its worth to your organisation. Various frameworks exist to accomplish this. Familiarity with the terms used is useful for developing your own classification systems.

Information Security issues to be considered when implementing your policy include the following:

- Inappropriate security classification of information may lead to disclosure of highly confidential information into the public domain, resulting in a loss of reputation for your organisation.
- Lack of a standardised classification system will result in inconsistent application of this policy.
- Lack of awareness of the organisation's standard classification procedures will result in information being classified inappropriately.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.2 Information classification

Policy 140106
Accepting Ownership for Classified Information

SUGGESTED POLICY STATEMENT

"All information, data and documents are to be the responsibility of a designated information owner or custodian."

EXPLANATORY NOTES

All information or data should belong to a person who is authorised to handle that information, and that person is normally responsible for its safe keeping.

Information Security issues to be considered when implementing your policy include the following:

- Confidential information apparently not owned by any one person could become lost, amended or compromised resulting in potential loss or embarrassment to the organisation.
- If information owners or custodians are unaware of the procedures for handling sensitive information, it could become available to unauthorised persons.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

5.1.1 Inventory of assets
5.2 Information classification

Policy 140107
Managing Network Security

SUGGESTED POLICY STATEMENT

"Access to the resources available from the organisation's network must be strictly controlled in accordance with the agreed Access Control List, which must be maintained and updated regularly."

EXPLANATORY NOTES

The level of security controls applied to a network must at least match the highest level of classification of the data being transmitted. The choice in the type of network will depend on many factors including cost, flexibility and security requirements.

Information Security issues to be considered when implementing your policy include the following:

- Classified data may be intercepted whilst travelling over a network (data taps), resulting in the loss of information, which may have a detrimental effect on your organisation's business.
- If suitable access controls are not implemented on the network, it is very likely that unauthorised persons may gain access to information.

RELATED ISO 17799 AND BS 7799 REFERENCE(S)

8.5.1 Network controls
9.4 Network access control

GLOSSARY AND REFERENCE MANUAL

Introduction

The terms listed within this Glossary and Reference represent a varied selection of the terms used in the world of IT, Security, and Business, all of which have some connection with the subject of Information Security - even if only tenuous. These words, phrases, expressions, acronyms, and abbreviations, are used in everyday conversation, as well as in various reference texts, and may well be encountered in conferences, seminars, broadcast and print media, and other situations.

While some of the terms such as '**Masquerading**' derive from the normal use of English vocabulary, others such as '**Hose and Close**' are better described as 'slang', 'jargon', or 'technobabble'.

Not all of these terms need be taken with the utmost seriousness; there are one or two spots of light relief. Where appropriate (and if known!) we have indicated the source of the expression.

For a number of entries, we have felt it appropriate to include more detailed guidance. For example, whilst we exhort organisations to issue a **Request For Proposal** ('RFP') document, some may find it helpful to be guided as to its contents. Likewise, testing business software needs to be planned and rather than simply advise organisations to perform a '**User Acceptance Test**', we have provided real guidance on how this should be performed. We hope that this is seen as beneficial.

10Base-T

Twisted pair Ethernet cabling wire, able to transport data up to approx. 185 metres.

24x7

'Twenty Four by Seven' i.e. twenty four hours a day, seven days a week, (three hundred and sixty five days per year). i.e. 'non-stop', or 'open all hours'.

4004

In full the Intel 4004. The world's first microprocessor, released in 1971. The 4004 contained 2300 transistors and was intended for use in a calculator. By comparison, the 1996 Pentium Pro contained 5.5 million transistors, an increase of over 239,000% in 25 years - thereby helping to demonstrate Moore's Law.

404

More fully, '404 Not Found'. Originating from the HTTP error 'file not found on server', now extended to humans either to indicate that someone is not where they should be, (equivalent to the Military's 'AWOL'), or to convey that the subject has no idea or no clue - sapience not found.

42

The Answer to Life, the Universe, and Everything – but before the answer makes any sense, you have to know the question ! From the Hitch-hikers Guide to the Galaxy by Douglas Adams.

8.3

Eight dot three. The standard DOS file naming convention consisting of an eight character name and a three character extension intended to indicate the file type. Long file names are clearly easier to use and understand, but many older users mourn the passing of the fixed 8.3 approach since it instilled a mental discipline and forced users to produce a descriptive file name with limited characters.

Abend / Application Crash

Abend (derived from 'abnormal end') is where an applications program aborts, or terminated abruptly and unexpectedly. One of the prime reasons for a thorough testing of an organisation's applications systems is to verify that the software works as expected. A significant risk to your data is that, if an application crashes it can also corrupt the data file which was open at the time.

Abort

A computer is simultaneously running multiple programs, each of which require the execution of a number of processes, often simultaneously. However, processes will usually interact with other processes and, due to the differences in hardware and

load on the system, will execute at varying speeds. A process may abort when it fails to receive the expected input, or is unable to pass the output to a linked process.
When a process aborts, it has the same effect as though that process had crashed. Poorly written applications may freeze / hang when one or more processes abort.

Acceptance

The point at which the business end-users of a system declare, formally, that the system meets their needs and has performed satisfactorily during the test procedures. Unless a system has been acquired, installed, or amended, purely for IT department it is not sufficient for technical staff to declare it acceptable; the end users must be involved.

Access

Two types of access – Physical and Logical.

1. **Physical Access**. The process of obtaining use of a computer system, - for example by sitting down at a keyboard, - or of being able to enter specific area(s) of the organisation where the main computer systems are located.
2. **Logical Access**. The process of being able to enter, modify, delete, or inspect, records and data held on a computer system by means of providing an ID and password (if required). The view that restricting physical access relieves the need for logical access restrictions is misleading. Any organisation with communications links to the outside world has a security risk of logical access. Hackers do not, generally, visit the sites they are hacking in person.- they do it from a distance!

Access Control

Access control refers to the rules and deployment mechanisms which control access to information systems, and physical access to premises. The entire subject of Information Security is based upon Access Control, without which Information Security cannot, by definition, exist.

Access Control List

The Access Control List - ACL - is a file which a computer's operating system uses to determine the users' individual access rights and privileges to folders / directories and files on a given system. Common privileges allow a user to read a file (or all the files in a folder / directory), to write / update the file or files, and to run (execute) the file (if it is an executable file, or program).

Access Rights

The powers granted to users to create, change, delete, or simply view data and files within a system, according to a set of rules defined by IT and business management. It is not necessarily true that the more senior a person, the more power is granted. For example, most data capture - essentially creating new files or transactions, is performed at relatively junior level, and it is not uncommon for senior management to have access rights only to view data with no power to

change it. There are very good Internal Control and Audit reasons for adopting this approach.

Accidental Damage

In relation to Information Security, accidental damage refers to damage or loss, that is caused as a result of a genuine error or misfortune. However, despite the genuine nature of the accident, such incidents can, and should be prevented by awareness, alertness and action.
For example, whilst we can all sympathise with the person who has lost their 50 page document through a system crash, there is little excuse for not having made a suitable backup copy from which to recover the situation.

Account

An 'account' is the term used most commonly to describe a user's profile which permits access to computer systems. Sometimes the account refers simply to the means of gaining network access to printers and the filing system; in other instances 'accounts' can be application systems' specific and incorporate a range of optional privileges controlling a user's level of access. (See Access Control).

Achilles Heel

The term Achilles Heel refers to an area of weakness which, when applied to Information Security means the weak link in the security safeguards. An example of an Achilles Heel would be where substantial effort has been made to secure data on the server, and yet virtually anyone is able to walk in to the systems room and remove the disk sub-systems.
The appropriate action for the Security Officer in your organisation, is to identify the Achilles Heel, and to take action against it.

Admissible Evidence

Admissible Evidence is 'evidence' that is accepted as legitimate in a court of law. From an Information Security perspective, the types of 'evidence' will often involve the production of a system's log files. The log file will usually identify the fact that a login took place; and certain functions were performed. The issue as to whether or not such a log file is legally admissible, is **not** clear cut. However, opinion appears to be that as long as a computer record is generated as a normal part of business processing, and the computer and software were working as designed and expected, then it may be admissible. Advice from a lawyer is always recommended.

ADSL

ADSL (Asymmetric Digital Subscriber Line) is a relatively new technology for transmitting digital information at high speeds, using existing phone lines (POTS) to homes and business users alike. Unlike the standard dialup phone service, ADSL provides a permanent connection, at no additional cost.
ADSL was specifically designed to exploit the one-way nature of most multimedia communication in which large amounts of information flow toward the user and

only a small amount of interactive control information is returned. Several experiments with ADSL to real users began in 1996. In 1998, wide-scale installations began in several parts of the U.S. In 2000 and beyond, ADSL and other forms of DSL are expected to become generally available in urban areas. With ADSL (and other forms of DSL), telephone companies are competing with cable companies and their cable modem services.

N.B. The Information Security implications of connecting full time to the Internet should not be underestimated. Anyone connecting their system full time to the Internet, needs a firewall, which does not have to cost $hundreds.

Agent

A piece of software performing some function on behalf of its user; usually independently, remotely, and unattended. See Crawler.

AI

Artificial Intelligence The holy grail of IT folk, the concept of a machine thinking for itself. Don't hold your breath.

Alpha Geek

The most knowledgeable, technically proficient, person in an office, work group, or other, usually non-IT, environment. Born 'fiddlers' and 'tinkerers', they tend to ignore the basic rule of 'If it ain't broke don't fix it' preferring to operate on the basis of 'Fix it, until it is broke'. Such people can be a considerable security risk - like ordinary Geeks, Anoraks, and Tech-heads, - only more so.

Alpha Software

Software, described as an 'alpha version' means that, whilst it has received basic testing by the developer(s), it is not yet ready for full testing. Alpha versions may have modules or components missing or with only partial functionality. Alpha software should **never** be used for other than demonstrations and (elementary) testing.

Analog, Analogue

A description of a continuously variable signal or a circuit or device designed to handle such signals. The opposite is 'discrete' or 'digital'. Typical examples are the joysticks or steering wheels associated with flight and driving simulations or air/space combat games.

Analogue Computer

A machine or electronic circuit designed to work on numerical data represented by some physical quantity (e.g. rotation or displacement) or electrical quantity (e.g. voltage or charge) which varies continuously, in contrast to digital signals which are either 0 or 1 (Off or On).

For example, the turning of a wheel or the movement of a mouse or joystick can be used as input. Analogue computers are said to operate in real time and are used for research in design where many different shapes and speeds can be tried out quickly. A computer model of a car suspension allows the designer to see the effects of changing size, stiffness and damping.

Analyst

In two basic IT variants - Business Analysts, and Systems Analysts - these individuals are involved in the front end design stages of systems from the view points of users and IT respectively. The analysts will determine the business requirements to be addressed, the processes which are involved in meeting those needs, and the systems designs which will deliver those requirements to the users.

Anoraks

Whimsical term for computer enthusiasts - usually, but not exclusively, young and lacking in social skills. The term derives from the preferred item of apparel for attending computer exhibitions, it being equipped with numerous sizeable pockets ready to be stuffed with all manner of obscure electronic gizmos.
Some anoraks tend more to the software side of IT and may graduate to being Hackers. Anoraks certainly have their uses but, in many ways, are a security risk. Such persons are inclined to do things with, and to, organisation IT systems simply for the technical and intellectual challenge, rather than for any business benefit to the organisation. Also known as Nerds, Geeks, and Tech-heads, the term is acquiring wider usage to describe any enthusiastic follower of obscure sports, hobbies, pastimes, etc.

ANSI

American National Standards Institute which is the main organisation responsible for furthering technology standards within the USA. ANSI is also a key player with the International Standards Organisation – ISO.

Anti-Virus Program

Software designed to detect, and potentially eliminate, viruses before they have had a chance to wreak havoc within the system, as well as repairing or quarantining files which have already been infected by virus activity

Application

A computer system, program, or set of programs.

Application software

Computer programs that are used by the Organisation to meet its business needs (as opposed to system software). Typically such software includes programs for accounting, transaction processing, word processing, spreadsheets, databases,

graphics, and presentations, and any special software developed specifically for that particular business.

Archie

Deriving from Archive, Archie is a system to gather, index and serve information on the Internet automatically. The initial implementation of Archie by McGill University School of Computer Science provided an indexed directory of filenames from all anonymous FTP archives on the Internet. Later versions provide other collections of information.

Architecture - Technical and Applications

The term 'technical architecture', refers to the core technologies deployed across a computing resource / network. For example an organisation's technical architecture may comprise UNIX servers running on RISC hardware, Windows® NT servers running on Intel CISC processors; over a 100BASE-T network using CAT 5 cabling.
The application's architecture can refer to a range of components but, in the corporate environment, identifies the foundational database upon which the majority of business applications are built. For example an organisation's applications architecture could be Oracle relational database (running on the UNIX servers identified above in the technical architecture) for business applications, and Microsoft Office® for all office and inter-organisation communications.

Archive

An area of data storage set aside for non-current (old, or historical) records in which the information can be retained under a restricted access regime until no longer required by law or organisation record retention policies. This is a field in which computers have a distinct advantage over older paper files, in that computer files can be 'compressed' when archived to take up far less space on the storage media. Paper records can only be compressed by using microfilm, microfiche, or, more recently, by scanning into a computer system. Whichever system is chosen, care must be exercised to ensure that the records retained meet legal requirements should it ever be necessary to produce these records in a court of law.

Archiving

The process of moving non-current records to the Archives. Once records are no longer required for day-to-day operations they should be passed to the control of an independent Archivist

Archivist

Individual (or possibly, department) responsible for the retention, care and control, and subsequent destruction, of non-current records. The Archivist should be independent, not involved in processing, and have no power to create or amend records other than registers/indices of stored material.

ARP – Address Resolution Protocol

When data arrives at a local gateway, bound for a specific local computer, ARP will map the inbound IP Address to the local machines physical address – know as its MAC address.

ASP

1. **Application Service Provider**. An ASP rents software to users and provides access over the Internet, instead of selling it outright. Despite the initial enthusiasm for ASPs in 2000, the Information Security issues that are raised by running software (with corporate data) across the Internet, cannot be under-estimated.
2. **Active Server Pages**. Active Server Pages are Web pages (HTML pages) embedded within which, are (small) programs, or scripts, which run just before the page is delivered to the user.

Audit Log

Computer files containing details of amendments to records, which may be used in the event of system recovery being required. The majority of commercial systems feature the creation of an audit log. Enabling this feature incurs some system overhead, but it does permit subsequent review of all system activity, and provide details of: which User ID performed which action to which files when etc.
Failing to produce an audit log means that the activities on the system are 'lost'.

Audit Trail

A record, or series of records, which allows the processing carried out by a computer or clerical system to be accurately identified, as well as verifying the authenticity of such amendments, including details of the users who created and authorised the amendment(s).

Auditor

Person employed to verify, independently, the quality and integrity of the work that has been undertaken within a particular area, with reference to accepted procedures.

Authentication

Authentication refers to the verification of the authenticity of either a person or of data, e.g. a message may be authenticated to have been originated by its claimed source. Authentication techniques usually form the basis for all forms of access control to systems and / or data.

Authorisation

The process whereby a person approves a specific event or action. In companies with access rights hierarchies it is important that audit trails identify both the creator and the authoriser of new or amended data. It is an unacceptably high

risk situation for an individual to have the power to create new entries and then to authorise those same entries themselves.

Auto Dial-back

A security facility designed to ensure that 'dial up' links to the organisation's communications network may only be accessed from approved/registered external phone numbers. The computer holds a list/register of user IDs and passwords together with telephone numbers. When a remote call is received from one of these users the computer checks that ID and password match and then cuts off the connection and dials back to the 'registered' telephone number held in the computer files. This system works well with fixed locations such as remote branches but may be inconvenient for staff who move around a lot. The drawbacks may be overcome by using a mobile telephone (connected to a laptop computer) as the registered dial-back - subject to the security requirements of protecting such items against theft or eavesdropping.

Availability

Ensuring that information systems and the necessary data are available for use when they are needed. Traditionally, computer systems were made available for staff use by the IT department in the early morning, and then closed down again by the IT staff before running their 'End of Day' routines. Availability was thus the poor relation of Confidentiality and Integrity in security terms. However the extension of the working day (for example because of trading with different time zones) and the growth of 24x7 systems, associated with e.g. web sites, Internet (on-line) trading, cash point machines, coupled with the threats of viruses and intrusions means that availability has become a much more important element of Information Security work.

Back Door

1. A back door is the name given to a 'secret' access route into the system. Such routes are usually undocumented and almost certainly were not originally specified. In fact, usually only the original developer would be aware of the back door(s) to their system. So why design a back door? Some boffin programmers, suspected that the end users would, at some point, make such a mess of the system, that normal ID and password routines would not allow access, and that another route into the system (known **only** to the programmers) would be required - the back door.

   In this particular context the existence of a Back Door can be a useful feature but, it does represent a significant risk in that a person - not necessarily on the staff of the organisation - could be in a position to penetrate the system with malicious intent without the organisation's knowledge. It is reasonable to assume that a programmer with sufficient skill to build the system in the first place will also have the skills necessary to penetrate the system and withdraw again without leaving any evidence of the incursion.

2. Name of several unpleasant viruses/Trojans which jeopardise network security and attempt to give malicious users access to the computer.

Backup

The process whereby copies of computer files are taken in order to allow recreation of the original, should the need arise. A backup is a spare copy of a file, file system, or other resource for use in the event of failure or loss of the original. The term is most commonly used to refer to a copy of all the files on a computer's disks which is made periodically and kept on magnetic tape or other removable medium (also called a 'dump').
This essential precaution is neglected by most new computer users until the first time they experience a crash or accidentally delete the only copy of the file they have been working on for the last six months.
Ideally the backup copies should be kept at a different site or in a fire safe. Although hardware may be insured against fire, the data on it is almost certainly neither insured nor easily replaced. Consequential loss policies to insure against data loss can be expensive, but are well worth considering.

Backup and Restore / Recovery

Whilst backup is a routine that is well understood, the ability to restore data is usually only performed when data is lost, corrupted, or otherwise changed. It is extremely important to review and test the restore procedures, to ensure that, in an emergency, appropriate action can be taken. A real danger, when restoring files from the backup, is that of restoring additional files which then over-write newer files. Were this to happen to an order processing system, or other system which records transactions, such an error could result in severe loss.
To avoid even the possibility of such an error, you should always restore files to a specific location that is separate from the live files. Then, having verified the integrity of the restored file(s), they may be copied to the required area; again, cautiously and with consideration for the risks involved.

Backup Files

Backup files are those files which are retained, often on high capacity tape or separate disk sub-system, which represent the organisation's protection against loss, damage or non-availability of the data held on information systems.
Whilst it is important to have available the most recent few backups - to enable restore in case of need - it is also crucial that recent backup tapes / disks are stored safely off-site; sufficiently far away to reduce the risk of environmental damage (e.g. flood) destroying both the primary systems **and** the off site backups.

Backup Power Generators

Backup Power Generators are usually gasoline driven units which are linked to an Uninterruptible Power Supply (UPS), to prevent your systems crashing as a result of power failure. Power generators should be of adequate capacity to support the systems which require power. Bear in mind that backup power generators are used rarely. As a result, they can remain idle for years, as usually the UPS will bridge

the gap until the power is either restored, or the systems have been safely shut down. As a result, when needed, the power generator may not have been tested for a considerable period. It is important that, periodically, the power generator is tested and serviced, in accordance with the manufacturer's recommendations. It is also vital to ensure that fresh gasoline replaces unused gasoline each year; and that there are adequate supplies available.

Batch

1. A term from the days before real-time processing when data was collected together throughout the day in batches waiting for the IT staff to run the End of Day routines which included 'batch processing'. This approach requires less computer power than real-time processing since account balances and other record are not changed until the end of the working day and, effectively the system is on 'enquiry only' status until the next processing run. In some ways batch processing is more secure than real-time since there is more time to check transaction data before it reaches the computer's files, however the advantages of having accurate, up-to-the-minute information (especially in banking and finance) are generally viewed as outweighing any benefits batch processing may offer.
2. Batch files (files with the extension .bat) are small 'programs' instructing the computer to perform some processing, start another program running, recognise some hardware etc., The most common example is the autoexec.bat file (standing for AUTOmatic EXECution) found on virtually every PC which runs each time the PC is started.

BBS

Bulletin Board System/Service. Prior to the 1990s and the explosive growth of the World Wide Web, systems' users were offered a direct dial-up link to the supplier's BBS, from which they could download files and/or read hints, tips etc. BBS access is now less common as all such sites have migrated to the Web.

Bench Testing

The testing of new / revised software by the developers. Bench testing is a critical step in the software development process and precedes the more 'formal' User Acceptance Testing process.
Bench testing should verify that the software performs in accordance with System Requirements.

Bespoke

In the same way as this term means 'made to measure' in clothing, it is used generally to describe software which has been written/developed specifically for one organisation. Bespoke differs from 'Customised' in that customisation usually refers to modification of existing software rather than starting from scratch.

Beta Software

Term used to describe software which is almost fully developed but not yet quite ready for release to the market, or internal users. The Beta version of the software is preceded by the alpha version. Beta versions of commercial programs are often made available to consumers at attractive prices on the basis that there are numerous bugs still to be sorted out, and the first batches of users to install the product are, effectively, taking part in an enormous acceptance testing programme. The developer will take note of the findings and comments made by Beta users to incorporate modifications, fixes, patches, etc., in the version which is finally released.
Beta versions of software, whether purchased or developed in-house, should not be installed on live systems and should never be used for mission critical processes.

Big Blue

Affectionate nickname for IBM, deriving from the colour of their hardware.

Binders

Binders are programs that allow hackers to 'bind' two or more programs together to result in a single .EXE file. These may be useful tools but they easily allow a hacker with malicious intent to insert Trojan executables into harmless .EXE animations, e-greetings and other .EXEs that are commonly passed around as e-mail attachments.
'The only way to stop an executable from harming your PC is to run it in a proactive 'sandbox' environment and monitor its behaviour for malicious activity in real-time.'

Biometric Access Controls

Security Access control systems which authenticate (verify the identity of) users by means of physical characteristics, e.g. face, fingerprints, voice, or retina pattern.

BIOS

BIOS, the Basic Input Output System of a personal computer. The BIOS contains the code which results in the loading (booting) of a computer's operating system e.g. Microsoft Windows®. The BIOS also controls the flow of data to/from the operating system and peripheral devices, such as printer, hard disk, keyboard and mouse.

Bitloss

Loss of data bits during a transmission. Such losses are usually self evident when the incoming file is reviewed, but, occasionally the loss is such that it goes unnoticed. Bit loss can be counteracted by use of Control Totals.

Black Magic

A technique that works, though nobody understands why. The positive version of a JOOTT.

Bloatware

Software that provides minimal functionality while requiring a disproportionate amount of diskspace and memory. Especially used for application and OS upgrades. This term is very common in the Windows/NT world. So is its cause.

Blue Screen of Death

Commonly abbreviated to BSOD, this term is closely related to the older Black Screen of Death but much more common. Due to the extreme fragility or 'bugginess' of the Microsoft Windows® 3.1/3.11 of the early 1990s, and early versions of Windows® 95 / 98, misbehaving applications can crash the system. The Blue Screen of Death, sometimes decorated with hexadecimal error codes, is what you get when this happens. The only solution is to re-boot and hope that it doesn't happen again (but it always does!). Solution: use a more stable operation system. If Microsoft Windows® compliance is key, which it normally is for most Small to Medium Sized Enterprises), consider Windows® 2000 professional or server.

BMUS

Beam Me Up, Scotty. From the original Star Trek series, now used as a plea for help by any techie in a tight spot. Also the source of the term 'Beam'.

Boeing Syndrome

The ultimate disaster scenario for contingency planning purposes. The name, allegedly, comes from a conference in which IT specialists, administrators, planners, etc were asked first to imagine that a Boeing 747 Jumbo fell out of the air onto their computer centre (with the resulting complete loss of systems) and then asked to prepare a contingency/disaster recovery plan to keep their organisation going in such circumstances. A very useful exercise - even for small companies, who often do not realise just how important their computer systems are to their continued existence as a viable business.

Boot

Starting up a PC or server. Verbal shorthand for 'Kick it 'til it wakes up'. The origin of this (strange) term is the recognition that booting or, system start up, is a process requiring a piece of 'bootstrap' code in the BIOS of the computer, which starts the loadup of the operating system.

Boot Disk

CD-ROM or Floppy disk used to start a PC or server when it cannot do so from the hard drive. Boot disks are often used when there is a problem with a Hard Drive,

but, equally, may be used as a Key Disk security feature when a PC has been deliberately configured by technical staff to refuse to run without the Key Disk present.

Borg

From 'Star Trek: The Next Generation' in which the Borg is a species of cyborg that ruthlessly seeks to incorporate all sentient life into itself; their slogan is 'Resistence is futile. You will be assimilated.' In tech-speak, the Borg is usually Microsoft, which is thought to be trying just as ruthlessly to assimilate all computers and the entire Internet into itself - there is a widely circulated image of Bill Gates as a Borg - ie Borging the competition. Being forced to use Windows or NT is often referred to as being 'Borged'. It is reported that this term is in use within Microsoft itself. Other companies, notably Intel and UUNet, have also occasionally been equated to the Borg.

Bot

Short for Robot, - the term describes little programs designed to perform automated tasks on the Internet such as indexing, looking/watching for message contents, or to act as avatars (human surrogates). On IRC, Bots can be malicious by cloning themselves, (clonebots), or flooding the IRC channels with garbage (floodbots). There are hundreds of different types of Bots including, by some definitions, Agents and Crawlers.

Botrunner

A person who operates software robots on the Net.

Bottlenecking

Also known as Mail Bombing, and similar in nature to Spamming and Flaming, Bottlenecking involves material being sent electronically to a organisation's access points (typically E-mail servers) in such large quantities that the system becomes blocked, and genuine business material cannot get through - for example sending ten full copies of the complete Encyclopaedia Britannica to all known E-mail addresses at an organisation will choke quite a few LAN servers for a good while. Although the material itself may not be inflammatory or abusive the senders usually have a grudge of some kind, real or imagined, against the organisation, and the end result is a organisation which cannot communicate with the outside world for an unknown period of time.

bps

bits per second. This is a term from which you can gauge the relative speed of a modem and / or network. Modern modems all offer at least 56K bps whilst the more modern ADSL lines are promoting 512K bps for home users and 2M bps for business users. The faster, the better, especially for Internet Web browsing.

Brochureware

Planned but non-existent product similar to vapourware, but with the added implication that marketing is actively selling and promoting it – i.e. they've printed brochures. Brochureware is often deployed as a strategic weapon alongside the pre-emptive announcement; the idea is to con customers into not committing to an existing product of the competition. It is a safe bet that when a brochureware product finally becomes real, it will be more expensive than and inferior to the alternatives that had been available for years. Typically market leader Organisation A will hear/see that competitor Organisation B has a superb new product likely to take market share from A. Organisation A therefore announces its own version and prints the brochures (while covertly reverse engineering/decompiling etc., B's product) so that existing customers will keep their brand loyalty and hold off buying from B. If successful enough, the brochureware can drive B out of the market, and B, together with its product range can be taken over by A. This part of the process is known as 'Borging'.

Brooks' Law

'Adding manpower to a late software project makes it later'.

Browser

Often known as a 'Web Browser', it is software used to make contact with Web sites on both the Internet and internal Intranets. The topic of software houses development and use of Browsers is controversial, and lies at the heart of the US Government anti-trust (monopoly) case against Microsoft. The only real effect of this case upon users is likely to be that, in future, Browser applications will have to be acquired and installed separately, rather than being supplied as part of an operating system.

BS 7799

The British Standard for Information Security which was re-issued in 1999 in two parts. Part 1 is the Code of Practice for Information Security Management and Part 2 specifies the requirements for implementing Information Security in compliance with the Code of Practice.
In October 2000, BS 7799 was elevated to become an International Standards Organization (ISO) standard – ISO 17799.

Bug

A fault in a computer system, usually associated with software. The term apparently stems from the early (pre-transistor) days of computing when machines used myriad valves and miles of wire. An apocryphal tale has it that one machine refused to work and, on examination of its innards, revealed a moth which had expired across some terminals thereby causing a short circuit. Once 'debugged' the machine worked perfectly - or so it is said.
These days the term is used indiscriminately to describe any situation in which a system behaves differently to expectations, and it is a generally accepted view that

ALL commercially available software contains bugs - they just haven't discovered them all yet.Business Assets
The term Business Assets, as it relates to Information Security, refers to any information upon which the organisation places a measurable value. By implication, the information is not in the public domain and would result in loss, damage or even business collapse, were the information to be lost, stolen, corrupted or in any way compromised.
By identifying and valuing the business assets in an organisation, and the systems which store and process them, an appropriate emphasis may be placed upon safeguarding those assets which are of higher value than those which are considered easily replaceable – such as information in the public domain.

Business Assets

The term Business Assets, as it relates to Information Security, refers to any information upon which the organisation places a measurable value. By implication, the information is not in the public domain and would result in loss, damage or even business collapse, were the information to be lost, stolen, corrupted or in any way compromised.

By identifying and valuing the business assets in an organisation, and the systems which store and process them, an appropriate emphasis may be placed upon safeguarding those assets which are of higher value than those which are considered easily replaceable - such as information in the public domain.

Business Case

The Business Case forms the foundation for any proposed venture or project. It establishes (in commercial / business terms) the need, justification and proposed alternatives to resolving a business issue or strategic objective. It is the Board of Directors, or most senior members of the organisation, who will demand, receive, review and (eventually) 'sign off' the Business Case.
The Business Case will discuss the alternative solutions explored and the conclusions reached. It will identify the risks of each alternative and establish the economic justification for the proposed course of action. In addition, it will project future returns to justify the cost of the project or venture.
The Business Case is a document which should be updated at key milestones during the project's lifecycle. It should be used as a probe and test through which changing circumstances are 'filtered' to ensure that the fundamentals and key objectives of the project remain valid. Where discrepancy is found, the Business Case should be updated to reflect the current circumstances, and the direction of the project modified where so required.
The Business Case should **not** be a document which is written by the IT department in an effort to gain acceptance for the latest IT upgrade! A Business Case is written by 'the business' or commercial side of the organisation, **but** often with strong support and input from the IT section / department to aid with the (inevitable) technical aspects of the proposal.

Business Continuity Plan - BCP

BCP – Business Continuity Plan. This is a plan to ensure that the essential business functions of the organisation are able to continue (or re-start) in the event of unforeseen circumstances; normally a disaster of some sort. However, BCP is not to be confused with Disaster Recovery Planning which is focussed upon crisis management.
Having dealt with the immediate crisis: securing the health and safety of people and preventing further spread or continuation of the crisis (e.g. a fire), the Disaster Recovery Plan will hand over to those responsible for executing the Business Continuity Plan.
The BCP will identify the critical people (roles / functions), information, systems and other infrastructure, e.g. telephones, which are required to enable the business to operate. The BCP will lay out a detailed plan which, if called upon, should be executed to assure minimum additional disruption.

Business Process Reengineering - BPR

Business Process Reengineering (BPR) is the development (and / re-development) of business procedures based upon the identification of the underlying business process. BPR should ignore 'vertical' departmental structures and identify the processes which generate value for the customer.
Unfortunately, "BPR" has developed a rather negative meaning; primarily because the dream, or vision, was but rarely realised, and many projects failed to deliver other than a large cost!
BPR was brought into the commercial spotlight in 1990 by Michael Hammer in his thought provoking article "Reengineering work: don't automate, obliterate," (Harvard Business Review 68 (4, July-August): 104-112). From this was generated a huge wave of enthusiasm based upon the achievements of some of the largest names in Corporate America.
More than a decade has now passed, and BPR has matured. It is now recognised that BPR is not simply about new processes and new technology, it is about the transformation of the organisation from the (traditional) vertical, 'stove pipe', departmental based organisation, to one that is based around core processes with process owners driving the business. This is not simply a matter of semantics – it is a fundamental change in approach, holding at its core, the creation of customer value as the primary objective for all and any business and organisation.

Business Requirements

The needs of the business processes which must be addressed by either a manual or computerised system. It is critical that the business requirements be clearly defined and documented, otherwise other issues may take its place, such as the recommendations of the IT group or supplier, which has a valid, but separate agenda. In many cases, business owners and managers find it seemingly complex to document their needs beyond high level requirements.
However, by recalling the tenets of Information Security, the high level requirements may be refined further by specifying the needs of the system with respect to, **Confidentiality** - who is able to see / amend what, **Integrity** - a system that is proven, tested and has security and fall back routines in case of

need; and **Availability** – the system must be available (say) to users in multiple offices both on workstations and on their laptops.
The Business Requirements is a statement about what matters and the priority of those issues. Time spent in agreeing these is never time wasted.

Capacity Planning

Capacity Planning is the determination of the overall size, performance and resilience of a computer or system. The detailed components of a Capacity Planning initiative will vary, depending upon the proposed usage of the system, but the following should always be considered :-

- the expected storage capacity of the system and the amount of data retrieved, created and stored within a given cycle.
- the number of on line processes and the estimated likely contention.
- the required performance and response required from both the system and the network i.e. the end to end performance.
- the level of resilience required and the and the planned cycle of usage – peaks, troughs and average.
- the impact of security measures e.g. encryption and decryption of all data.
- the need for 24x7 operations and the acceptability of downing the system for maintenance and other remedial work.

When capacity planning, the more information available about usage patterns and overall systems' loading, the better. Recently, with the exponential increase in Internet Web site usage, the results from any Capacity Planning have been, at best of limited use, and at worst, useless. The reason is because, it has been almost impossible to predict the possible volume of traffic (hence load) with the result that many sites have simply gone down under the excessive load conditions. Therefore, Capacity Planning needs to consider the real possibility of excess load scenarios and plan accordingly. (but there are no easy answers).

CCTV

Close Circuit Television, used as a security device and also a deterrent around office buildings, stores, campus sites, etc. CCTV cameras will usually have their output recorded onto video tape to enable any suspicious activity to be subsequently reviewed.

CD / CDROM

Since their introduction in the early 1980s, CDs – Compact Disks - have gradually replaced the older vinyl disks as a means of music storage. However, whilst the term 'CD' was adopted for CDs which store music, the term CD-ROM (CD Read Only Memory) was adopted by the computer word, despite using the same optical disks. Ironically, the term CDROM still persists despite the fact that CD read / writers have been available for years.

CERT

CERT – the **C**omputer **E**mergency **R**esponse **T**eam, is recognised as the Internet's official emergency team. It was established in the USA by the Defense Advanced Research Projects Agency (DARPA) in 1988 following the Morris computer Worm incident crippled approximately 10% of all computers connected to the Internet. CERT is located at the Software Engineering Institute - a US government funded research and development centre operated by Carnegie Mellon University - and focuses on security breaches, denial-of-service incidents, provides alerts and incident-handling and avoidance guidelines.
CERT is also the publisher of Information Security alerts, training and awareness campaigns. CERT may be found on the World Wide Web at www.cert.org.

Certification Authority

A trusted third party clearing house that issues Digital Certificates and Digital Signatures. Such certificates include your organisation's name, a serial number, and an expiry date. In addition, and to allow for the encryption and decryption of data, the public key of your organisation. Finally, the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is valid.
The following companies provide various levels of certification services for organisation's and individuals alike : VeriSign, Entrust, Baltimore Technologies, and Thawte.

Challenge

Sometimes referred to as a 'Challenge Handshake' or 'Challenge Protocol', this is an enquiry signal/message transmitted by a computer, being contacted by another machine, for that machine to identify itself and/or its user. The computer equivalent of 'Halt, who goes there?' An acceptable response from the calling machine will allow contact to proceed, whilst failure to satisfy should result in termination of the communication connection.

Change Control

An internal control procedure by which only authorised amendments are made to the organisation's software, hardware, network access privileges, or business process etc. This method usually involves the need to perform an analysis of the problem and for the results to be appended to a formal request prepared and signed by the senior representative of the area concerned. This proposal should be reviewed by management (or committee) prior to being authorised. Implementation should be monitored to ensure security requirements are not breached or diluted.

Chat Room

A feature of the Internet allowing users to 'talk', in real time, through a keyboard to one or more persons in a 'virtual environment'. Recent reports of viruses being transmitted through messages in Chat Rooms have raised the security profile of

such activities, and organisation's are advised to review the ability of staff to access such facilities.

Checksum

Checksum is a technique whereby the individual binary values of a string of storage locations on your computer are totalled, and the total retained for future reference. On subsequent accesses, the summing procedure is repeated, and the total compared to that derived previously. A difference indicates that an element of the data has changed during the intervening period. Agreement provides a high degree of assurance (but not total assurance) that the data has not changed during the intervening period.
A check sum is also used to verify that a network transmission has been successful. If the counts agree, it is safe to assume that the transmission was completed correctly.

Cipher

A cipher is the generic term used to describe a means of encrypting data. In addition, the term *cipher* can refer to the encrypted text itself. Encryption ciphers will use an algorithm, which is the complex mathematical calculation required to 'scramble' the text, and a 'key'. Knowledge of the key will allow the encrypted message to be de-crypted.

CISC / RISC

Complex Instruction Set Computer, refers to the instruction set (or pre-programmed commands) within microprocessors. Those from Intel's Pentium processors are referred to as CISC because they have a full and comprehensive instruction set; whereas those from IBM, powering their RS6000 mini-computers, are RISC – Reduced Instruction Set.

Clear Desk Policy

A Policy of the organisation which directs all personnel to clear their desks at the end of each working day, and file everything appropriately. Desks should be cleared of all documents and papers, including the contents of the 'in' and 'out' trays! The purpose of the Clear Desk Policy is not simply to give the cleaners a chance to do their job, but to ensure that sensitive papers and documents are not exposed to unauthorised persons out of working hours.

Clear Screen Policy

A Policy of the organisation which directs all users of screens / terminals to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentially. Typically, the easiest means of compliance is to use a screen saver which will engage, either on request, or after a specified time.
See also Shoulder Surfers.

Clerical Systems

Also known as Manual Systems, or Manual Processing, these are business processes that do not rely on computers for their successful completion.

Client

A computer system or process that requests a service from another computer system or process, a 'server'. A client is part of a client-server software architecture
For example, a workstation requesting the contents of a file from a file server is a client of the file server.
'Thin Client': A simple client program or hardware device which relies on most of the function of the system being in the server. By the mid-1990s, the model of decentralised computing where each user has his own full-featured and independent microcomputer seemed to have displaced a centralised model in which multiple users use thin clients (e.g. dumb terminals) to work on a shared minicomputer or mainframe server. Networked PCs typically operate as 'fat clients', often providing everything except some file storage and printing locally. By 1996, the reintroduction of thin clients was being proposed, especially for LAN-type environments. The main expected benefit of this is ease of maintenance: with fat clients, especially those suffering from the poor networking support of some operating systems, installing a new application for everyone is likely to mean having to go physically to every user's workstation to install the application, or having to modify client-side configuration options; whereas with thin clients the maintenance tasks are centralised on the server and so need only be done once. Also, by virtue of their simplicity, thin clients generally have fewer hardware demands, and are less open to being sabotaged by 'ambitious' Lusers.

Client-Server

A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to some protocol, asking for information or action, and the server responds.
This is analogous to a customer (client) who sends an order (request) on an order form to a supplier (server) who despatches the goods and an invoice (response). The order form and invoice are part of the protocol used to communicate in this case.
There may be either one centralised server or several distributed ones. This model allows clients and servers to be placed independently on nodes in a network, possibly on different hardware and operating systems appropriate to their function, e.g. fast server/cheap client.

CMYK

Cyan, Magenta, Yellow, blacK. The four colours of ink used by computer printers. The letter K is used for Black to avoid confusion with the B of RGB.

CODEC

- **CO**der/**DEC**oder An integrated circuit or other electronic device combining the circuits needed to convert digital signals to and from analogue form.
- **CO**mpression **DEC**ompression - a technique used to reduce the size of files as they are transmitted and then expanded to normal size at the receiving point. This process is automatic, requiring no user intervention. CODECs improve transmission speeds and reduce the risk of data manipulation during transmission.

Command Line

The command line refers to the blinking cursor which, prior to the use of Microsoft Windows®, is at the heart of all operating systems. In the world of mini computers and UNIX®, the command line is often called the '$' prompt and signifies that the operating system is able to accept another command; e.g. to 'mount' a new disk-pack or to format a disk.
People familiar with Microsoft DOS environment will always recall the 'C' prompt, being the command line familiar to all PC users as C:\ (with optional parameters to include the current path).

Commission

The commissioning of a (computer) system is the point when it is put into live, operational, and active service.

Common Gateway Interface – CGI

CGI is a programming method of passing information between a Web site and an applications programme and back again. CGI applications can be written using a variety of programming languages e.g. Perl (from UNIX), C, C++, Visual Basic and others.
There are significant security risks in implementing CGI scripts using scripting languages such as Perl, because, although extremely powerful for the manipulating and parsing of text (say from user input), they also permit an array of low level 'system' commands which could be exploited for malicious purposes.

Communications Equipment

Hardware, with associated software, relating to the ability of computers to receive data from, and transmit data to, locations separated from the central processor.

Communications Line

Within a communications network, the route by which data is conveyed from one point to another. Recently the term has started to be replaced by 'Communications Link' to reflect the fact that a growing number of small networks, even within the same building, are using radio ('wireless') communications rather than fixed cables.

Communications Network

A system of communications equipment and communication links (by line, radio, satellite, etc.,), which enables computers to be separated geographically, while still 'connected' to each other.

Compression

A technique, using special software, to increase the storage capacity of computer media, either by artificially increasing the apparent size of a computer disk, or reducing the size a files stored thereon. Compression comes in two flavours; Disk Compression and File Compression.
Disk Compression dates from the mid-1980's when hard drives were very much smaller and, relatively, much more expensive than today. A typical 1990 hard drive would store 80 Megabytes of programs and data, compared to the year 2000 'basic' home user specification of 4.3 Gigabytes (4,300 Megabytes) - an impressive growth of 5,275%. As a result of vastly increased disk storage capacities, users' enthusiasm for such techniques has, not surprisingly, waned somewhat. Overall, it is generally regarded as being cheaper and easier to install another hard drive than deal with the drive/file structures and performance degradation often associated with disk compression. Companies with computer archives dating back to 1995, and earlier, should review these archives to ensure that the files thereon can still be accessed by the systems and software now being used and, if necessary, give consideration to decompressing such disks and storing the information on new, larger capacity, disks.
File compression, conversely, is being used more frequently. Commonly referred to as 'Zipping' after the most popular compression programs (PKZip, and WinZip) this increase in usage is due in no small part to the increasing use of electronic transmission systems to move files between remote parts of the organisation, and even around the world at large. A typical Word Processor document can be compressed by 90% or more and thus a file of 1 Megabyte can be reduced to 100 Kilobytes. Sending a zipped file not only reduces the cost of transmission, by taking less time to transmit, but also, by the same token, reduces the risk of transmission error. Companies should be aware, however, that unattractive elements such as viruses can be contained within compressed files, ready to activate themselves as soon as the file is decompressed. Consequently, any Anti-Virus software selected by the organisation should be capable of detecting viruses within a compressed file before it is decompressed and brought into the system.

Compressors / Packers

Compressors, or Packers are legitimate compression utilities which will compress (make smaller) Windows® program files - .EXE files. In a similar way to using a popular file compression utility such as WinZip before e-mailing, compressors do the same for executable files. However, unlike WinZiped files, which require to be decompressed before loading, compressed executables run in their new state. **Because of this, the executable will pass through any anti-virus scanning engine because the virus signature has been modified and the anti-virus software will not recognize it**.

There are many free and available compression utilities and these have been responsible for many of the Trojan variant programs and worms which have caused so much damage. Here are a few examples of common compressors, AS-pack, PECompact, Petite, PKLite, NeoLite, Shrinker and WWpack32.
With such compressed files being able to circumvent your anti-virus software, what options are available? According to one hackers site, “The only way to stop an executable from harming your PC is to run it in a proactive "sandbox" environment and monitor its behaviour for malicious activity in real-time.”

Computer Abuse

Precursor of Computer Crime; the first reported instance occurred in 1958!

Computer System

One or more computers, with associated peripheral hardware, with one or more operating systems, running one or more application programs, designed to provide a service to users.

Computer Viruses

Computer Viruses are pieces of programming code which have been purposely written to inflict an unexpected result upon an innocent victim. There are now approximately 50,000 viruses and their variants for which known cures of ‘vaccines’ are available.
Viruses are transmitted within other (seemingly) legitimate files or programs, the opening, or execution of which, causes the virus to run and to replicate itself within your computer system, as well as performing some sort of action. Such actions can be as harmless as causing characters to ‘fall off’ the screen (early DOS based Virus in the 1980s), to the most malicious viruses which destroy data files and replicate themselves to everyone in your e-mail directory.
It is essential to guard against virus attacks by a combination of cautious, guarded, awareness, together with a modern anti-virus package and regular updates – every two weeks is recommended.
There are many Internet sites providing updates on Viruses; here are some examples www.sophos.com or www.symantec/avcenter.

Confidentiality, Integrity and Availability

A key aspect of Information Security is to preserve the confidentiality, integrity and availability of an organisation’s information. It is only with this information, that it can engage in commercial activities. Loss of one or more of these attributes, can threaten the continued existence of even the largest corporate entities.
Confidentiality. Assurance that information is shared only among authorised persons or organisations. Breaches of Confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, e-mailing or creating documents and other data etc. The classification of the

information should determine is confidentiality and hence the appropriate safeguards.
Integrity. Assurance that the information is authentic and complete. Ensuring that information can be relied upon to be sufficiently accurate for its purpose. The term Integrity is used frequently when considering Information Security as it is represents one of the primary indicators of security (or lack of it). The integrity of data is not only whether the data is 'correct', but whether it can be trusted and relied upon. For example, making copies (say by e-mailing a file) of a sensitive document, threatens both confidentiality and the integrity of the information. Why? Because, by making one or more copies, the data is then at risk of change or modification.
Availability. Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

Console

The console, is the screen and keyboard which allows access and control of the server / mainframe in a networked environment. The console will usually be within a secure area with access only granted to system's administrators, with all actions being logged.
Users of the console will usually have highly privileged access such as Systems Operations, Super User or root.

Consumables

The 'stationery' items, such as ink cartridges, toner, and paper, which are required for production of the output from a computer system, and which must be replenished regularly.

Contention

Contention manifests itself in a slowing or reduction in response from a system. The cause of the problem results from increased loading on a system or network, such that requests for information and / or processing, are queued within the internal buffers of the system. Where contention becomes extreme, the buffers can overload and the system can fail / crash.
To reduce contention, and hence reduce the risk of system overload, an analysis of the load will need to be performed. An example of contention leading to overload was in mid 2,000 in the UK, where a leading Bank launched its e-Banking service. Within hours of the opening, the service was down due to massive contention and overload; concurrent demand had exceeded capacity by an unexpected order of magnitude. See Capacity Planning.

Contingency Arrangements

A set of formally approved, detailed plans and procedures specifying the actions to be taken if or when particular circumstances arise. Such plans should include all eventualities ranging from key staff absence, data corruption, loss of

communications, virus infection, partial loss of system availability, etc., through to the complete disaster Boeing Syndrome.
The increased use of computers in the business world make such plans essential.

Contingency Planning

In project management, a valuable lesson learnt early in one's career is :-

'A failure to plan, is a plan to fail'

Contingency planning, plans for the unexpected or, the possibility of circumstances changing. Contingency plans are individual plans associated with individual projects or programmes.
A contingency plan is never expected to be executed; as result, where attention to detail and the budget allocation are clearly inadequate, this can guarantee its failure in the event of it being executed.
As with any plan, it is essential to agree the 'trigger(s)' which will result in the plan coming into force and the subsequent 'chain of command' which will take over during that period.
See also Business Continuity Planning.

Control Total

A value that can be compared against the sum of a batch of items to check against loss in transit. Similar to old-style test keys, the system can compare what the control total indicates was transmitted with the incoming records of what was actually received. If the control total is transmitted separately from the transactional message(s) to which it relates, it can provide some protection against fraudulent or mischievous manipulation of data in transit. The safest way of using control totals is to send the control total message at a different time, and by a different route to the master message.

Controls

Procedures, which can reduce, or eliminate, the risk of a threat becoming an incident.

Cookie

A small identifier file placed on a user's computer by a Web site, which logs information about the user and their previous/current visits for the use of the site next time the user makes contact. The Web site owners claim that this is beneficial to the user, allowing faster access, and 'personalisation' of the site for that user.
Growing numbers of users are less than entirely happy with the idea of a remote machine placing spurious files on their system, which may contain personal information including user IDs and passwords - especially when a credit card has been used for purchasing goods or services on-line. There is no obvious benefit to the user - the speed gains are marginal at best, and some users are now setting

their browsers to reject Cookies, or deleting any received during the day, at close of business. For more information, visit www.cookiecentral.com/

Copy Protection

Techniques used by software developers to (try to) prevent illegal use of their products. The unlicensed use of software (i.e. software piracy) is a major problem. It is not difficult for an organisation to purchase, say, one licensed copy of a program and then install it on, say, 6 separate machines. Or install the program on a server and allow numerous users access through a network. **This is illegal**, rendering the organisation liable to prosecution - **even if the installation was carried out without management's knowledge**.

Copy Protection comes in a number of forms :-

Moral; a legal copy comes with an End User Licence Agreement (EULA) which states the terms upon which the software may be used. The EULA usually includes a selection of dire threats concerning the possible actions which the software developers may take if unauthorised use of the software comes to their attention.

Physical, typically a Dongle or a Key Disk, one of which is supplied with the original program and must be physically present on/in a computer before the program will run. Quite effective but unpopular with users since, typically, a parallel or serial port or floppy drive will be used by the device, and hence is unavailable for other use.

Required Input; method used most commonly in games software, whereby the program will not run until it has been give a specific piece of information which is (or should be) available only to the registered user. Typically this will be a particular word from a specific place in the official user manual, or a number from a code sheet. One copy of the manual or code sheet will have been supplied with the software and the required input will change each time the program is started. This approach is quite effective, but since the manual may often easily be scanned also, it is not full proof.

Logical; a variety of methods used singly or in combination, including non-standard formats of disks (to dissuade copying), machine-specific registration, installation counters, etc designed to minimise the risk of the program being installed on more than one machine.

Copyright

The UK Copyright, Designs and Patents Act, 1988 states that "the owner of the copyright has the **exclusive** right to copy the work". The function of copyright is to protect the skill and labour expended by the author, of a piece of work. As such, copyrighted material may not be printed, copied or distributed without permission from the owner of the copyright. In general, you cannot copyright facts but the consequential analysis, presentation and approach can certainly be copyrighted. Especially when information is downloaded from the Internet, it is dangerous to assume that it is in the 'public domain' unless it is explicit on the point.

As soon as the author creates a 'work' (of whatever nature) which is **original**, a copyright automatically come into existence. The author is not obliged to register the work, although registration makes the copyright more visible.

To avoid any misunderstanding, all documents, reports, surveys etc should have the copyright owner affixed.

Corrupt Data

Data that has been received, stored, or changed, so that it cannot be read or used by the program which originally created the data. Most common causes of corrupt data are disk failures (usually where the magnetic coating of the disk is breaking down, and the computer cannot read the disk properly) and power failures, where the computer loses power and shuts down unexpectedly with random writes to the hard drive, and loss of memory contents.

Cracker

A cracker is either a piece of software (program) whose purpose is to 'crack' the code to, say, a password; or 'cracker' refers to a person who attempts to gain unauthorised access to a computer system. Such persons are usually ill intentioned and perform malicious acts of techno-crime and vandalism.

- **Code breaking software**. A piece of software designed to decipher a code, but used most often to 'crack a password. Crackers operate quite simply by testing large numbers of possible passwords much faster than a human being could hope to perform. Passwords can be extraordinarily complex, but, given sufficient time, and sufficient computer power, ANY password can be broken - even one of 64 case-sensitive characters. Companies are well advised to ensure that, to prevent system penetration by a Cracker, there is a limit on the number of password tries permitted before the system locks and notifies the Security Officer and/or Network Administrator. Three attempts is fairly standard; other systems may be less strict, while some high security installations will permit only one attempt before locking and generating security alert messages.
- **Illegal entry into a computer system**. These individuals often have malicious intent and can have multiple tools for breaking into a system. The term was adopted circa 1985 by hackers in defence against journalistic misuse of hacker. Contrary to widespread myth, cracking does not usually involve some mysterious leap of intuition or brilliance, but rather the persistent repetition of a handful of fairly well-known tricks that exploit common weaknesses in the security of target systems. Accordingly, most crackers are only mediocre hackers. Crackers tend to gather in small, tight-knit, very secretive groups that have little overlap with the huge, open hacker poly-culture; though crackers often like to describe themselves as hackers, most true hackers consider crackers a separate and lower form of life, little better than virus writers.

Crash

System Failure, often accompanied by loss of data. The term stems largely from the days of the first Hard Disks which were prone to physical damage. The gaps between the surface of the disk and the drive heads which read and write the data are so small (considerably less than the thickness of a human hair) that, if disturbed while in use, the heads would, literally, crash into the surface of the disk thereby ruining the surface and destroying program files and/or data. The heads

had to be 'parked' in a safe position before the disk pack or computer was moved. Manufacturing standards have improved dramatically since then, and true crashes are now quite rare, but the term remains as a general description of a system suddenly stopping for no immediately obvious reason.

Crawler

Also known as a Web Crawler, but sometimes described as an Agent, or a Bot. In essence a Crawler is a highly specialised search engine, designed to 'crawl' around the World Wide Web looking for particular pieces of information, addresses, references, etc., while the user is off-line, i.e. not connected to the Internet, and therefore not running up connection charges. The Crawler will search the Internet 24 hours a day, until the next time its user logs on, when the results/information obtained so far will be transmitted to the user, and the Crawler will continue. Although not necessarily benign, Crawlers are not usually malevolent - merely seeking information rather than actively damaging systems - although the information concerned may be sensitive, classified, or confidential.

Crippled

More commonly associated with software rather than hardware. The term indicates that the application is not capable of performing all functions normally expected of such a program, for example saving or printing files created by the user. Usually used in connection with shareware, or promotional software where some functions are deliberately crippled as an incentive for a user to pay for the fully-functional version.

Crippleware

Shareware, or promotional software, which has been crippled, i.e. some functions, such as printing or saving files, have been disabled by the developer. Whilst logical from the developer's perspective, its popularity has fallen, as it fails to allow the user to use the system properly and hence can avert sales, rather than promote them. Far better is the technique whereby the software is fully functional for, say, 30 days, and then refuses access until a licence string is entered. Even the removal of the software and a re-install will not result in a further 30 days. Why? - because the developers are smarter than that! Upon installation, a tiny hidden file is created in a secret location. This file and its contents are read upon start up, and thus the user is forced to make a purchase decision.

CRT

CRT stands for Cathode Ray Tube, and is the traditional means of displaying pictures on a monitor or television. Indeed, the old green monitors used with the first PCs were called CRTs. Today, workstation monitors still used an electron beam as the core technology, but newer 'flat screen' technologies are set to revolutionise screen technology.

Cryptography

The subject of cryptography is primarily concerned with maintaining the privacy of communications, and modern methods use a number of techniques to achieve this. Encryption is the transformation of data into another usually unrecognisable form. The only means to read the data is to de-crypt the data using a (secret) key, in the form of a secret character string, itself encapsulated within a pre-formatted (computer) file.

Customise

To modify a piece of standard software to suit some specific needs of the organisation. For example an accounting system developed to meet typical UK accounting requirements may need some customisation if bought by a user in a country with different accounting and reporting standards.
However, for such customisation to be possible would require, either access to the source code (unlikely, unless you developed it yourself, or are willing to buy the company), or are able to convince the software developers about the need to customise the software to meet your specific needs.

Cutover

Sometimes known as ‘going live’. Cutover is the point at which a new program or system, takes over – perhaps from a previous version, and the old program is no longer used. On major developments, this point is reached when the new software has been written, tested, and run satisfactorily, in parallel with the old, for an agreed period.

Cybercrime

Cyber crime is any criminal activity which uses network access to commit a criminal act. With the exponential growth of Internet connection, the opportunities for the exploitation of any weaknesses in Information Security are multiplying. Cyber crime may be internal or external, with the former easier to perpetrate. The term has evolved over the past few years since the adoption of Internet connection on a global scale with hundreds of millions of users. Cybercrime refers to the act of performing a criminal act using cyberspace (the Internet network), as the communications vehicle. Some would argue that a Cybercrime is not a crime as it is a crime against software and not against a person’s person or property. However, whilst the legal systems around the world scramble to introduce laws to combat Cybercriminals, two types of attack are prevalent :-

- **Techno-crime**. A pre-meditated act against a system or systems, with the express intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts or all of a computer system. The 24x7 connection to the Internet makes this type of Cybercrime a real possibility to engineer from anywhere in the world; leaving few if any, ‘finger prints’.

- **Techno-vandalism**. These acts of 'brainless' defacement of Websites, and/or other activities such as copying files and publicising their contents publicly, are usually opportunistic in nature. Tight internal security, allied to strong technical safeguards should prevent the vast majority of such incidents.

Cybersitter

Also Net Nanny, a Cybersitter is a piece of software, originally designed for parents concerned about their children's unrestricted access to the seamier side of the Internet, which can be used to block a users access to websites containing 'dangerous' or 'offensive' material.
Cybersitters are being used more widely, as companies realise that such material obtained by their staff and stored on a organisation computer could jeopardise system security as well as rendering the organisation liable to breaches of legislation, e.g. on defamation, data protection, the Official Secrets Act, morality, etc.
Conversely, to avoid the problems of civil/human rights breaches, constructive dismissal, labour tribunals, etc, companies need to exercise caution when dealing with staff found to be making 'inappropriate' use of Internet and E-mail facilities. The dice are loaded.

Cyberwar

Alternative name for Infowar.

Cybrarian

Contraction of Cyber-Librarian;

1. an individual responsible for care and control over, and extraction of data from, the organisation's computer archives and electronic reference libraries.
2. an individual skilled (and possibly making a legitimate living) at obtaining information electronically from on-line sources in various parts of the Internet.

Data / Information

In the area of Information Security, data (and the individual elements that comprise the data) is processed, formatted and re-presented, so that it gains meaning and thereby becomes information. Information Security is concerned with the protection and safeguard of that information which, in its various forms can be identified as Business Assets or Information Assets.
The terms data and information can be used somewhat interchangeably; but, as a general rule, information always comprises data, but data is not always information.

Data Capture

The process of entering data into a computer system. This can be a manual process where data is entered through a keyboard, or by scanner, or other equipment, or may be automatic where a system is receiving a transmission from another program or computer.

Data Classification

Data Classification is the conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted. The classification of the data should then determine the extent to which the data needs to be controlled / secured and is also indicative of its value in terms of Business Assets.
The classification of data and documents is essential if you are to differentiate between that which is a little (if any) value, and that which is highly sensitive and confidential. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level. For many organisations, a simple 5 scale grade will suffice as follows :-

Document / Data Classification	Description
Top Secret	Highly sensitive internal documents e.g. pending mergers or acquisitions; investment strategies; plans or designs; that could seriously damage the organisation if such information were lost or made public. Information classified as Top Secret has very restricted distribution and must be protected at all times. Security at this level is the highest possible.
Highly Confidential	Information that, if made public or even shared around the organisation, could seriously impede the organisation's operations and is considered critical to its ongoing operations. Information would include accounting information, business plans, sensitive customer information of bank's, solicitors and accountants etc., patient's medical records and similar highly sensitive data. Such information should not be copied or removed from the organisation's operational control without specific authority. Security at this level should be very high.
Proprietary	Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organisation operates. Such information is normally for proprietary use to authorised personnel only. Security at this level is high.

Document / Data Classification	Description
Internal Use only	Information not approved for general circulation outside the organisation where its loss would inconvenience the organisation or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level is controlled but normal.
Public Documents	Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level is minimal.

Data Encryption

Data encryption is a means of scrambling the data so that is can only be read by the person(s) holding the 'key' – a password of some sort. Without the 'key', the cipher cannot be broken and the data remains secure. Using the key, the cipher is decrypted and the data is returned to its original value or state.
Each time one wishes to encrypt data, a key from the 72,000,000,000,000,000 possible key variations, is randomly generated, and used to encrypt the data. The same key must be made known to the receiver if they are to decrypt the data.
See Cryptography and DES/AES.

Data Mart

A Data Mart, in contrast to a Data Warehouse, is a database of information collected from operational and other systems, which is made available to a group of users to meet a specific Business Need. The presence of a Data Mart often suggests the presence of a Data Warehouse, but not necessarily so. In general, a Data Warehouse tends to be implemented for strategic long term reasons, whereas a data mart tends to be tactical and directed at meeting an immediate business need.

Data Mining

1 Data Mining is the analysis of corporate data, for relationships and correlations which have yet to be discovered. Such relationship discoveries can identify significant marketing opportunities to target specific client segments. The term Data mining was coined by IBM who hold some related patents.

2 Spending numerous hours combing the Internet looking for specific pieces of information, and finding everything except what you are looking for!

Data Safe

A Safe made of heavy, fire-resistant, tamper-resistant, magnetically inert, materials. Datasafes are usually dual controlled, and are designed for the safe keeping of computer media, including master program media, 'mission critical' software, and top security data files.

Data Warehouse

The term Data Warehouse, or Information Warehouse, refers to a specific type of database – in terms of both hardware and software, the sole purpose of which is to store and execute searches upon, substantial volumes of corporate data. A data warehouse is not, or should not be, a larger version of the organisation's current transaction processing system. A Data Warehouse should be a separate data store that is optimised for the type of data and queries envisaged.

Database

A collection of files, tables, forms, reports, etc., held on computer media that have a predictable relationship with each other for indexing, updating, and retrieval purposes.

Database Administrator – DBA

A 'DBA' is a highly technical person who has specialised in the development and maintenance of databases and database applications. The DBA is responsible for ensuring that all housekeeping routines are performed on the database, which may include designing and maintaining the structure and content of the (many) tables which together form the database, and the relationships between these tables. In addition, the DBA will usually be specialised in writing reports and querying the database, usually using Structured Query Language – or SQL.

Datascope

An electronic device that is capable of detecting and reading the bit-patterns of data passing down a communications line and interpreting/translating these patterns into readable alphanumeric characters.
Some devices are capable of detecting/reading the electromagnetic radiation emitted directly by computers without the need to 'tap' a communications line.

Dead Tree Edition

Techie slang for 'Hard Copy' - i.e. anything printed on paper, rather than held on computer media.
An ironic reference to the source of the paper required.

Debug

To trace and fix faults (bugs) in computer software and, occasionally, hardware. The term derives from the same source as Bug.

Deciplegic

Mouse Potato suffering from Trigger Finger.

Decryption

The process by which encrypted data is restored to its original form in order to be understood/usable by another computer or person.

DED

Dark-Emitting Diode (non-functioning Light Emitting Diode), a Friode.

Default

A default is the setting, or value, that a computer program (or system) is given as a **standard setting**. It is likely to be the setting that 'most people' would choose. For example, the default font on your word processor maybe Times New Roman 10 pitch; unless you change this, it will remain at the default setting.
Defaults are used throughout the computer industry to enable software to work 'out of the box' and not require ordinary people ('Users') to spend hours selecting every conceivable option in advance - quite thoughtful really!

Default Password

The password installed by a manufacturer and required to access a computer system when it is initially delivered, or a password required by software (typically shareware) to prove that the user is registered with the software vendor. Default passwords are not normally encountered on new PCs and have become relatively rare, but, in cases where such a password has been installed, the new owner of the equipment should change it at the earliest opportunity, to avoid it being known to third parties.
There are a range of default passwords known to everyone; and these are the first ones tried by anyone hacking into, or merely attempting opportunistic access. Such passwords as 'password', '123456' and ' ' i.e. blank (nothing) must be

changed immediately. If you have one of these or similar passwords; please change it **now. *RUSecure™*** will still be here when you have finished!

Denial of Service

A Denial of Service (DoS)attack, is an Internet attack against a Web site whereby a client is denied the level of service expected. In a mild case, the impact can be unexpectedly poor performance. In the worst case, the server can become so overloaded as to cause a crash of the system.
DoS attacks do not usually have theft or corruption of data as their primary motive and will often be executed by persons who have a grudge against the organisation concerned. The following are the main types of DoS attack :-

- **Buffer Overflow Attacks**; whereby data is sent to the server at a rate and volume that exceeds the capacity of the system; causing errors.
- **SYN Attack**. This takes places when connection requests to the server are not properly responded to, causing a delay in connection. Although these failed connection will eventually time out, should they occur in volume, they can deny access to other legitimate requests for access.
- **Teardrop Attack**. The exploitation of a features of the TCP/IP protocol whereby large packets of data are split into 'bite sized chunks' with each fragment being identified to the next by an 'offset' marker. Later the fragments are supposed to be re-assembled by the receiving system. In the teardrop attack, the attacker enters a confusing offset value in the second (or later) fragment which can crash the recipient's system.
- **Smurf Attack or Ping Attack**. This is where an illegitimate 'attention request' or **Ping** is sent to a system, with the return address being that of the target host (to be attacked). The intermediate system responds to the Ping request but responds to the unsuspecting victim system. If the receipt of such responses becomes excessive, the target system will be unable to distinguish between legitimate and illegitimate traffic.
- **Viruses**. Viruses are not usually targeted but where the host server becomes infected, it can cause a Denial of Service; or worse.
- **Physical Attacks**. A physical attack may be little more that cutting the power supply, or perhaps the removal of a network cable.

DES / AES

DES – The Data Encryption Standard and the AES - Advanced Encryption Standard are both data encryption standards for the scrambling of data to protect its confidentiality.
It was developed by IBM in co-operation with the American National Security Agency and published in 1974. It has become extremely popular and, because it used to be so difficult to break, with 72,000,000,000,000,000 possible key variations, was banned from export from the USA. However, restrictions by the US Government, on the export of encryption technology was lifted in 2000 to the countries of the EU and a number of other countries.

The AES - Advanced Encryption Standard, is a state of the art algorithm (developed by Rijndael) and chosen by the United States National Institute of Standards and Technology on October 2, 2000. Although selected, it will not become officially "approved" by the US Secretary of Commerce until Q2 2001. Meanwhile, products are already available which use the Rijndael algorithm within AES encryption tools. For example http://www.privatecrypt.com/int/.

Desktop

1. Verbal shorthand for Desktop Personal Computer, normally used to differentiate such a system from a 'Laptop' or portable PC.
2. In Windows 95®, and later releases, the screen visible on the computer monitor is known as the desktop and can be used to store programs and data as if it were a normal directory/folder. It is generally considered better practice to use the desktop as a place to store links to files and programs, rather than the files and programs themselves. This is partly because of the risk of accidental deletion, but - more importantly to companies – to avoid such files being visible to any curious passer-by.

Development Library

An area of the computer systems' fixed storage area which is set aside for the development of software, to minimise/avoid the possibility of conflict between an existing program and a new version.

Development Machine

An additional computer system, not part of the main processing system. Usually smaller than the main system, but similarly configured, the development machine is used for creating new software, amending existing software, and testing such creations and amendments to ensure that there is no possibility of the daily work and security of the main system being compromised by conflict between different versions of the same program. The development machine may also be used as a contingency standby machine, in case of failure of the main system. Companies unable to justify the costs of duplicate machines should use a Development Library within a partitioned area of the main system.

DHTML

Dynamic HyperText Markup Language. Contrary to its name, DHTML is not a new version of HTML - the Hyper Text Markup Language used to generate Web pages. DHTML is the combination of several browser features which, together, permit a Web page to be more 'dynamic'. Dynamic in this sense means the ability for the Web page to change its look and features after the page has been loaded; perhaps dependent upon the selection of various options. The recent versions of the most popular Web browsers all offer DHTML support.

Digital

Employing the binary system of numbers (1 and 0 only) for processing purposes.

Digital Certificate

A digital certificate is the electronic version of an ID card that establishes your credentials and authenticates your connection when performing e-Commerce transactions over the Internet, using the World Wide Web.
To obtain Digital Certificate an organisation must apply to a Certification Authority which is responsible for validating and ensuring the authenticity of requesting organisation. The Certificate will identify the name of the organisation, a serial number, the validity date ("from / to") and the organisation's Public Key where encryption to / from that organisation is required.
In addition, the Digital Certificate will also contain the Digital Signature of the Certification Authority to allow any recipient to confirm the authenticity of the Digital Certificate.
A global standard (X. 509 Public Key Infrastructure for the Internet) defines the requirements for Digital Certificates and the major Certificate Authorities conform to this. Such standards, and the integrity of the Certificate Authorities are vital for the establishment of 'digital trust', without which e-Commerce will never attain its potential.

Digital Signature

A digital signature is an electronic equivalent of an individual's signature. It authenticates the message to which it is attached and validates the authenticity of the sender. In addition, it also provides confirmation that the contents of the message to which it is attached, have not been tampered with, en route from the sender to the receiver.
A further feature is that an e-mail 'signed' with a digital signature cannot easily be repudiated; i.e. the sender is not able to deny the sending and the contents of the message; plus it provides a digital time stamp to confirm the time and date of transmission.
For a digital signature to be recognised, and acknowledged as something of integrity, it needs to be trusted by the recipient. It is for this reason that a Certification Authority will supply a digital signature to persons, the identity of whom, it has been able to verify; perhaps by having an Attorney's stamp on a document which validates the applicant's name, address, date of birth etc.
To provide greater digital trust, the Digital Signature is packaged with the certificate of the Certification Authority, and this too may be inspected for validity and expiration.
Most people expect digital signatures to totally replace the use of the ('old fashioned') pen and ink signature with orders and authorities being accepted via digitally signed e-mails, the contents of which may, or may not, be encrypted for additional security.
N.B. In July 2000, Digital Signatures became legally accepted in the United Kingdom under Section 7 of the Electronic Communications Act. In the USA

also, Congress approved the use of Digital Signatures for certain types of e-Business around the same time under the E-Sign Act. Because both Acts are extremely new, it is strongly recommended that legal advice be sought before reliance is placed upon this new legislation.

Digital Versatile Disk – DVD

Currently, these optical storage disks are being pioneered by the entertainment business; notably because the DVD is able to store a full length feature movie on a single CD size disk, with faithful reproduction of visual and audio quality.
DVD, with a capacity (using both sides of the disk) of approx. 17GB, will doubtless replace the present CDs / CD-ROMs with their 'modest' 670MB capacity. At present consumer models are read only, but they will soon offer full record capability with integration into information systems.

Digital Watermark

A unique identifier that becomes part of a digital document and cannot be removed. The watermark is invisible to the human eye but a computer can analyse the document and extract the hidden data. Digital watermarks are being used for Classified/Top Secret documents - usually Military/Governmental - and highly confidential commercial material. The primary use of such marks is to allow different marks to be used when the document is copied to different persons and thereby establish an Audit Trail should there be any leakage of information.

Disable

The process by which hardware or software is deliberately prevented from functioning in some way. For hardware, it may be as simple as switching off a piece of equipment, or disconnecting a cable. It is more commonly associated with software, particularly shareware or promotional software, which has been supplied to a user at little or no cost, to try before paying the full purchase or registration fee. Such software may be described as 'crippled' in that certain functions, such as saving or printing files are not permitted. Some in-house development staff may well disable parts of a new program, so that the user can try out the parts which have been developed, while work continues on the disabled functions. Disabling is also often used as a security measure, for example the risk of virus infection through the use of infected floppy diskettes can be greatly reduced, by disconnecting a cable within the PC, thereby disabling the floppy drive. Even greater protection is achieved by removing the drive altogether, thereby creating a diskless PC.

Disaster Recovery Plan - DRP

The master plan needed by technical and non-technical staff to cope with a major problem - such as the Boeing Syndrome. Do not confuse and merge the DRP with the Business Continuity Plan. The DRP is the plan which is activated when there is

an emergency. It is the plan which ensures that health and safety come first followed by damage limitation. Having contained the impact of the disaster, and having ensured that the situation is now under control e.g. through the Emergency Services, then the Business Continuity Plan will be activated.
One of the most difficult aspects of a DRP is agreeing when it should be activated. In some circumstances it will be clear. For example, a tornado destroys part of the office block; or a serious fire reduces the premises to ashes. However, on many occasions, disasters have multiple warnings or indicators, and it is these which need to be considered and identified as the triggers to invoke your DRP.

N.B. The skills required to prepare and manage a DRP are not necessarily the same as those required for a Business Continuity Plan.

Distributed Processing

Spreading the organisation's computer processing load between two or more computers, often in geographically separate locations. If a organisation has the necessary financial and technical resources, distributed processing, with mirroring between sites, is an excellent contingency plan for sudden disasters.
Even if there is a total loss of one system, the remaining computer(s) can carry the load without disruption to users and without loss or corruption of data.

DMZ

A DMZ – De-Militarised Zone, is a separate part of an organisation's network which is shielded and 'cut off ' from the main corporate network and its systems. The DMZ contains technical equipment to prevent access from external parties (say on the Internet) from gaining access to your main systems.
The term comes from the buffer zone that was set up between North Korea and South Korea following their war in the early 1950s. A DMZ is not a single security component; it signifies a capability. Within the DMZ will be found firewalls, choke and access routers, front-end and back-end servers. Essentially, the DMZ provides multi-layer filtering and screening to completely block off access to the corporate network and data. And, even where a legitimate and authorised external query requests corporate data, no direct connection will be permitted from the external client, only a back-end server will issue the request (which may require additional authentication) from the internal corporate network.
However, the extent to which you permit corporate data to be accessible from and by external sources will depend upon the value of the Business Assets which could be placed at (additional) risk by allowing access to (even) pre-specified data types.

DNS

Domain Name System (or Server). The DNS is the means by which user friendly Web addresses are translated into arcane IP addresses. The DNS ensures that your are routed to the correct site.

Domain Name

The domain name identifies the location of an organisation or entity on the Internet and, through Domain Name Service translates this to an IP Address, which is the real address to which traffic destined for that domain name is routed.

Dongle

A mechanical device used by software developers to prevent unlicenced use of their product. Typically, a Dongle is a small connector plug, supplied with the original software package, which fits into a socket on a PC - usually a parallel port, also known generally as the LPT1 Printer port. Without the Dongle present, the software will not run. Some older Dongles act as a terminator, effectively blocking the port for any other use, but later versions have a pass-through function, allowing a printer to be connected at the same time. Even though the PC can still communicate with the printer, there have been problems with more recent printers which use active two-way communications with the PC to notify printing status, ink levels, etc.

Down

In IT terms, when a system is down, it is not available to users. This is not necessarily due to hardware or software faults, it may well be necessary to disconnect non-IT users, or take the system down for maintenance, installation of new hardware, loading new software etc. Traditionally such activities would take place after the End of Day, but the advent of 24x7 processing means there is no natural break in the cycle, and IT staff will therefore schedule the work for the time of minimum system workload - probably around 03:00 on Sunday morning!

Downtime

The amount of time a system is down in a given period. This will include crashes and system problems as well as scheduled maintenance work. Obviously, downtime impacts upon system availability, and most IT departments will maintain a downtime log to record when, and why, the system was not available to users. This log should be reviewed at intervals to identify any recurring problems, failure patterns etc.

DPI

Dots Per Inch. A measure of resolution for equipment such as printers and scanners. The more the better.

Drill Down

Descending through numerous layers of consolidations, summaries, etc., etc., to reach the really detailed information at the bottom.

Driver

A driver is a small interface program which allows a computer to communicate with a peripheral device, such as a printer or a scanner. The driver will be automatically installed when you connect the device to the PC; hence the need for a CD-ROM or floppy disk when installing such peripherals.

Dual Control

A control procedure whereby the active involvement of two people is required to complete a specified process. Such control may be physical; e.g. two persons required to unlock the Data Safe, or logical; as in the case of a higher level authorisation password required to permit the entry of data created or amended by another person.
Dual Control is one of the foundations of Information Security as it is based upon the premise that, for a breach to be committed, then both parties would need to be in collusion and, because one should always alternate the pairs of people, it would require a much greater level of corruption in order to breach dual control procedures; especially is such procedures require nested dual control access, such that (say) 2 pairs of people are required to enable access.
If this procedure appears someone 'dated' in today's 21st century 'wired' environment, please note that in 2000 a number of vendors started to sell 'Trusted Operations Systems', which enforce the requirement for dual control and the separation of duties, to provide substantially greater Information Security.

Dumb Terminal

A type of terminal that consists of a keyboard and a display screen that can be used to enter and transmit data to, or display data from, a computer to which it is connected. A dumb terminal, in contrast to an intelligent terminal, or PC, has no independent processing or storage capability and thus cannot function as a stand-alone device.

e-

Widely used - now widely overused - abbreviated prefix indicating 'electronic'. Given the current frenzy for on-line services, companies are sticking the 'e-' prefix onto the front of almost any word to show how progressive and technologically advanced they are :-
e-business, e-commerce, e-trading, e-finance, e-broking, e-shopping, e-retailing, e-money, e-cash, e-purse, e-wallet, - the list is (probably) endless.

Earwigging

Alternative (slang) term for Eavesdropping.

Eavesdropping

Listening to someone else's conversation. In its most basic form, it amounts to one person keeping within earshot of a conversation between two other persons, but in the security and IT worlds it extends to remote listening and recording devices, include the interception of telephone calls, fax transmissions, e-mails, data transmissions, data-scoping, and even radio scanning for mobile communications. The security implications for companies are primarily that user identification details or passwords can become known to criminally inclined individuals, or that confidential/sensitive information about the organisation, its finances, or activity plans may leak to competitors.

e-Business

Another term for e-Commerce.

e-Commerce

e-Commerce, e-Business or e-Tailing is an electronic transaction, performed over the Internet – and usually via the World Wide Web - in which the parties to the transaction agree, confirm and initiate both payment and goods transfer; at the click of the mouse.
There are two general types of e-Commerce activity; Business to Consumer (or Business to Customer) - B2C, and Business to Business – B2B.
Business to Consumer is usually, but not always, characterised by the purchase of goods or services, using the “shopping cart” metaphor and the acceptance of credit / debit cards in payment.
Business to Business, on the other hand, is concerned with using the Internet to place and receive orders from other businesses; establishing legally binding contractual commitments and pooling the resources of companies across the globe to tender for a project, with each party being authenticated and legally bound by their digital commitments.
However, to achieve this, and for e-Commerce to reach its true potential requires ‘digital trust’, and for this to take place requires strong technical tools to authenticate, encrypt and assure the confidentiality of data. Whilst e-Commerce can be initiated using e-mail, this requires the adoption of Digital Signatures which not only authenticates the sender, it also confirms the time and date of transmission and assures that the contents of the transmission were not tampered with.
Transactions initiated using Web servers, usually rely upon Digital Certificates and the use of the Secure Sockets Layer authentication and encrypted communication standard. In addition, to provide security for the secure transmission of documents, and other data, the use of the RSA standard is common, with Public

Key Infrastructure (PKI) being used to create, issue and manage the use of public and private keys (or Digital Certificates).

Editor

A program which allows a user to create, view, and amend, the contents of certain types of files. There are several types of editors, the most common being Text Editors, and Hex (Hexadecimal) Editors.
Editors work at the lowest level, either in ASCII (Text Editor) or directly with disk contents (Hex Editor).
Although text Editors, e.g. Notepad in Windows®, are common, companies should give consideration to staff access to Editors, particularly the more powerful types - such as Hex Editors. A Hex Editor can do considerable damage to the contents of computer files, which may not be recoverable.
N.B. Although Word Processors and other programs can be used to edit their own files, they are NOT Editors in this context.

EGA

Enhanced Graphics Adapter. Old style type of monitor. Great at the time (mid 1980s) – 'full colour' – but now several generations out of date.

Electronic Eavesdropping

Electronic eavesdropping is the intentional surveillance of data – voice, data, fax, e-mail, mobile telephones etc, often for nefarious purposes.

Electronic Mail - E-mail

Electronic Mail - an electronically transmitted message which arrives as a computer file on your PC or organisation's server. Originally conceived as a simple means of sending short messages from one computer to another, the Simple Mail Transfer Protocol (SMTP) was introduced without security in mind.
Whilst standards have been agreed for the attachment of files to e-mail messages, be aware that such files can contain malicious code such a virus. Use extreme caution when opening an e-mail message with an attachment; even if the e-mail is from someone you know; it is better to leave it unopened and enquire whether the e-mail is bona fide. If in doubt; destroy the e-mail and advise the sender that you have been unable to verify the authenticity of the attachment and to advise its contents. If in doubt; destroy the e-mail; if it's genuinely important, they will either make contact again or you have the option to send them an explanatory email.

Why is e-mail insecure ?

- An e-mail message can purport to have been sent from a specific individual, but the message **could** have come from someone else entirely. Anyone can set up an e-mail address with anyone else's name as the sender. e.g. a Mr. Bill Clinton

could easily setup and email address as George_Bush@hotmail.com. However, where email comes from a company or organisation, the user name is **likely** to have been setup centrally, with the opportunity for misrepresentation, less likely.

- Even where you have your own organisation's domain name e.g. email@myorganisationname.com, this too can be modified, such that the "From" field in the e-mail is sent with a fallacious sender; all designed to deceive the recipient.
- An e-mail message can be opened by anyone; and not only the intended recipient. There is no authentication such that only the intended recipients are able to read the mail. Like a postcard, an e-mail may be read by anyone who comes across it, either legitimately, or otherwise.
- The safe transmission of e-mail to its destination is not secure. Whilst the use of a "Read-Receipt" can be useful, especially using e-mail on Local Area Networks where network traffic is within known boundaries. E-mail sent across the Internet will pass through multiple computer nodes as it "hops" and "bounces" towards its destination address. However, even if it reaches its destination mail server, delivery to the recipient may be delayed or may not necessarily occur. Therefore, when e-mail is sent, even using a Digital Certificate, certified delivery to the recipient(s) is lacking. Best Practice is to request safe receipt from the recipient(s).
- It does not carry any legal validity. Unless sent using a Digital Signature an e-mail does not carry the legal validity as enjoyed by hard copy or signed fax transmission. However, legal reliance upon an e-mail sent using a Digital Signature cannot necessarily be relied upon as it was only in 2000 that the US and UK accepted that such e-mails **could** be used as legally binding documents.

E-mail Signature file

The e-mail 'signature' or .sig ('dot sig'), refers to the optional footer text appended to the end of each outward e-mail. Normally, a signature file includes the sender's name, and other contact details e.g. telephone number and Web site address.
It should also contain a disclaimer. Consider the following :

****

Email Confidentiality

Privileged/Confidential Information may be contained in this message. If you are not the addressee indicated in this message (or responsible for delivery of the message to such person), you may not copy or send this message to anyone. In such case, you should destroy this message and kindly notify the sender by reply e-mail.

****

It could also include a disclaimer about the possibility of spreading a computer virus :

****

Although this email has been scanned for the possible presence of computer viruses prior to despatch, we cannot be held responsible for any

viruses or other material transmitted with, or as part of, this email without our knowledge.
****
Where the contents of the e-mail are those which, despite being sent from a corporate e-mail system, are the **personal** views of the sender, and should therefore be detached from any possible corporate view on the subject, the sender may incorporate the following in their e-mail footer.
****
The opinions expressed above are my own and are not those of any company or organisation.
****

Encryption

The process by which data is temporarily re-arranged into an unreadable or unintelligible form for confidentiality, transmission, or other security purposes.

End of Day - eod

A set or routines, programs etc., performed/run by IT department staff after normal close of business. With the advent of 24x7 processing, such routines may well now be run during the early hours of the morning and would include, for example, taking backups, running interest accruals on closing balances, checking files integrity etc.

End User

Usually reduced simply to User. The person who actually uses the hardware or software that has been developed for a specific task.

End User License Agreement – EULA

The End User License Agreement – or EULA - is a legally binding contract between the developer or publisher of a software program (or application) and the purchaser of that software. However, unlike the purchase of goods or services, the EULA is, as its name implies, a license agreement. In other words, the purchaser does not own the software, they merely have a right to use it in accordance with the licence agreement.
During the install of package software, the purchaser is shown the contents of the EULA and is often required to scroll down through the EULA, at the bottom of which, one may Accept or Refuse the terms of the EULA. By enforcing the need to scroll through the EULA, a user would be unlikely to succeed in any action to deny acceptance of the terms of the EULA.
In some cases, the EULA is written on the outside of the packaging with the breaking of the seal to the CD, indicating acceptance of the EULA.

In all cases, the EULA is the contract which users ignore at their peril; and whilst most EULAs contains broadly similar clauses and restrictions, it is important to confirm these before committing your organisation.
Microsoft has helpfully provided detailed information about its own EULAs at www.microsoft.com/education/license/eula.asp.

Enforced Path

Normally, a user with the appropriate access control, is able to use any PC or workstation on the local area network to run an application or access certain data. However, where such data or system is classified as sensitive or requires restricted physical access, an enforced path may be applied. This is a straightforward configuration setting, performed by the Systems Administrator, whereby access is restricted to a specific workstation or range of workstations.
Enforcing the path will provide added security because it reduces the risk of unauthorised access; especially where such a workstation is itself within a secure zone, requiring physical access codes / keys etc.

Enhancement

In theory, an improvement in hardware or software over the current version. In practice, enhancements are often merely vehicles to introduce some 'new' features into a package before withdrawing support for the current product, thereby pushing users towards upgrading their systems - at a price.

Error Log

An error log records any abnormal activity on application software, usually in simple / plain text (ASCII). Each (main) application generates its own logs, and it is the responsibility of Systems Operations to retrieve and scrutinise them for any processing errors.

Escrow

A legal provision whereby, in the event of a developer/supplier failing or otherwise ceasing to trade, the source code for their packaged software is made available to licensed / registered users, thereby enabling its ongoing maintenance.

e-Trading

e-Trading is that part of e-Commerce which specialises in financial services. It deals in corporate paper (e.g. stocks and shares), the purchase of commodities, and currencies etc. It can be Business-to-Consumer or Business-to-Business.

Executable / .exe

The term ‘executable’ refers to a file that can be ‘run’ by a computer. Such software programs are usually identified by the suffix ‘.exe’. Executables are created when their source code is compiled and bound to the operating system upon which it is to be run.

Expectations Mismatch

Expectations mismatch refers to the all too common condition whereby the customer’s expectations are different from those of the supplier and is one of the most common reasons for systems projects to falter. No matter which project or initiative is concerned, **always** ensure that expectations remain synchronised throughout the project.
The seeds for such mismatch are normally sown early on in the project, where the vendor presents a solution to the need as they perceive it, and the organisation believes that the vendor’s system can meet their needs; such belief often being based upon the verbal assurances given by the vendor.
It is strongly recommended that, as negotiations are progressing, the organisation documents **precisely** what it expects each party to provide and, more importantly, what each is **not** expecting to do / provide.
Example : a major systems vendor contracted with a bank to deliver a new system where the vendor contracted to **implement** the system. The bank’s management, and its project team, understood this to mean ‘set up and configure the system, to enable us to use it’ (in a live environment). The vendor refuted this, and suggested that **implement** meant to load up the software and test that it was working. Any required support for a ‘migration to live operations’ would be at additional cost……. The project faltered and nearly failed.
Expectations mismatch occurs most often where plans are inadequate with the consequence that, when the detail tasks are to be performed, one or both parties presume that it is the responsibility of the other party and each then ‘points the finger’ at the other party. **Avoid this with a formal approach to project management**.

Expiry

The point/date by which an event (such as changing a password) must take place.

Extranet

An Extranet is a private network which uses the Internet protocols and extends beyond an organisation’s premises, typically to allow access by clients, suppliers, or selected third parties.
Extranets require strong security if they are to prevent unauthorised access. This can range from a relatively simple User ID and password to the use of Digital Certificates, User IDs and passwords, with, naturally, end to end encryption of data.

Fallback Procedures

Fallback procedures are particular business procedures and measures, undertaken when events have triggered the execution of either a Business Continuity Plan or a Contingency Plan.

Fax / Facsimile Machines

Whilst the use of faxes is being eclipsed by that of e-mail, they are still preferred where a legal record of transmission and delivery is required.
Fax machines operate by incorporating 3 technologies into a single unit : a scanner to convert a page into a graphical image; a printer to print the resultant image and a modem to transmit the data across the public telephone network. Despite the fact that fax images can be tampered with as easily as any other form of electronic data format, they have nevertheless become accepted as bona fide documents for legal purposes.
Great care should be exercised when accepting a fax as genuine because its Integrity may be questionable, as there is no data validation or authentication between sending and receiving parties. Any fax machine can use the Calling Station IDentifier (CSID) as it so wishes and, whilst some software can check the name of the CSID before transmission, this is of limited value where robust security is required.
Faxes should not be used for Confidential information where the Integrity of the information is paramount. In an effort to reduce the risk, callers and senders will often (physically) watch over the fax machine in order to capture the expected fax. However, it is 'wide open' from a security perspective and, because fax machine numbers are so publicly available, a 'tap' on the line could indeed intercept faxes.

Features / Glitches (Bugs)

Within the IT community, the term 'bug' is frowned upon, and is often replaced with the quaint term 'feature' or, a 'glitch'. Irrespective of how it is described, it remains a Bug !

Finagle's Law

The 'folk' version of Murphy's Law, fully named 'Finagle's Law of Dynamic Negatives' and usually rendered 'Anything that can go wrong, will.'. One variant favoured among hackers is 'The perversity of the Universe tends towards a maximum.'. The label 'Finagle's Law' was popularised by SF author Larry Niven in several stories depicting a frontier culture of asteroid belt miners. This 'Belter' culture professed a religion and/or running joke involving the worship of the dreaded god Finagle and his mad prophet Murphy.

Fire Fighters

Net users who attempt to put out, or at least damp down, Flames/Flame Wars before they get out of hand. Rarely successful.

Fire-Resistant Storage Cabinet

The legal records and documents of most organisations are likely to be in traditional paper / printer form. A fire resistant cabinet or safe is required to secure these documents from fire for a guaranteed period of time.

Firewalls

Firewalls are security devices used to restrict access in communication networks. They prevent computer access between networks (say from the Internet to your corporate network), and only allow access to services which are expressly registered. They also keep logs of all activity, which may be used in investigations. With the rapid growth in electronic communications - particularly via the Internet - firewalls, and firewall software, are being installed which will allow remote users to access limited parts of the system but restrict further access without satisfying specific identification and authorisation requirements. For example; an organisations' Web site will contain pages which are available to any Internet 'surfer' but other areas will not be accessible without recognition of authorised user status by the system. See Extranet.

Firewall Machine. A dedicated gateway computer with special security precautions on it, used to service outside network, especially Internet, connections and dial-in lines. The idea is to protect a cluster of more loosely administered machines hidden behind it from intrusion. The typical firewall is an inexpensive microprocessor-based Unix machine with no critical data, with modems and public network ports on it, but just one carefully watched connection back to the rest of the cluster. The special precautions may include threat monitoring, call-back, and even a complete iron box which can be keyed to particular incoming IDs or activity patterns.

Firewall Code. The code put in a system (say, a telephone switch) to make sure that the users can't do any damage. Since users always want to be able to do everything but never want to suffer for any mistakes, the construction of a firewall is a question not only of defensive coding but also of interface presentation, so that users don't even get curious about those corners of a system where they can burn themselves.

Firmware

A sort of 'halfway house' between Hardware and Software. Firmware often takes the form of a device which is attached to, or built into, a computer - such as a ROM chip - which performs some software function but is not a program in the sense of being installed and run from the computer's storage media.

Fit for Purpose

Fit for Purpose is a general expression which can be useful to ensure that Information Security solutions are appropriate for your organisation. Vendors will sometimes attempt to 'fit' their solution to your problem. Fit for Purpose is an expression which, when used within the solution negotiation context, places an onus of responsibility upon the vendor to ensure that its solution is (indeed) fit for the purpose which their client **expects**.
Example : a well known systems company contracted for the sale of their system. Inclusive in the price was one of week training in the system. During implementation it became apparent that one week for training was totally inadequate. The customer successfully claimed (prior to legal action) that the supplier's solution was inadequate and hence not **fit for purpose**.
When considering Information Security solutions, it is good practice to remind any potential suppliers in your requirement that the solution must be fit for purpose.
See also Request For Proposal.

Fix

An operational expedient that may be necessary if there is an urgent need to amend or repair data, or solve a software bug problem.

Fixed Storage

The internal media used by a computer to store files, data, programs etc, and usually referred to as the Fixed Disk(s) or Hard Drive(s). Fixed storage devices obviously can be removed from the system for repair, maintenance, upgrade etc., but generally this cannot be done without a toolkit to open up the system for physical access by an engineer. The term is used mainly to differentiate these items from removable storage media such as tapes, floppy diskettes, CDs, etc.

Flag

A message indication, sometimes, but not always, a warning to a user, which appears when a certain event takes place. For example, an inventory monitoring program may well 'flag' certain products when stocks fall below a predetermined level, to alert the user to re-order.
An alternative use is to warn of an event which will take place in the future, but has not yet occurred, for example, a financial institution aware of large cheque-based transaction on a customer's account may 'flag' the account to avoid an unauthorised overdraft.
Flags may be generated manually or automatically, depending on circumstances. In the case of the stock monitoring this would be automatic, while the cheque transaction example would be processed manually.
Automatic flags serve a useful purpose in drawing users' attention to situations which otherwise may be overlooked.

Flame

'Flame' is abusive communication by E-mail or posting to a newsgroup, which attacks an individual or organisation for some real or imagined grievance. The real problem is broader than that of a few rude e-mails: flame represents the anarchistic side of the Internet. The flame may start with only one abusive message, but it is broadcast so widely that large numbers of unconnected browsers join in - often on both sides of the argument. This can lead to 'Flame Wars', where the traffic load becomes so high that communications network performance degrades, and E-mail boxes become blocked - as is the case with bottlenecking and mail bombing.
Problems for companies may arise if a member of staff has used an organisation's e-mail address to start the flame - another reason to monitor staff activities.
Flame has some redeeming features. Deeply unpleasant (or disturbed) individuals who posted lengthy racist (or sexist, or some other -ist) diatribes have found themselves flamed off the Net….

Flame Bait

A Usenet posting or other message intended to trigger a flame war, or one that invites flames in reply. Acceptable for Usenet posters on a domestic machine, but not recommended in the office!

Flash

Two meanings. Firstly, Similar to a Flag but more obvious and usually more urgent, or more serious, a Flash is a visual warning to a user, often associated with security control procedures. For example, if a user who is already logged on at one computer attempts to also log on at a second terminal, the system will Flash the IT supervisor console to warn of possible attempted breach of security.
Secondly; Flash is a technology being used to provide complex animation and sound on Web sites. It is extremely popular!

Floppy disks

Floppy Disks are removable magnetic storage disks, used in personal computers and servers, to save data. Before 1987, floppy disks were 5.25 inches in diameter and flexible, hence the term 'floppy'. Despite the introduction of the 3.5 inch diskette in a hard plastic outer casing, the term 'floppy' still persists. In much of the IT world, their use has been almost totally replaced by CDs and Zip Disks. As of 2001, the re-writable 17GB Digital Versatile Disk (DVD) is available, which in turn replaces the CD (CD-ROM) and its 670 MB capacity.

Freeware

Literally, software provided for free - no charge. This is not as uncommon as might be expected. Major software developers often give away old versions of

their products to allow users to try them at no charge and, hopefully, succeed in tempting them to purchase the current release.
Independent developers may give away small programs to establish a reputation for useful software, which then enables them to charge. Cover disks attached to a computer magazine often contain Freeware.
As with Shareware, Freeware should be approached with caution, and staff dissuaded from trying out their new Freeware on organisation equipment.

Freeze / Hang

When an application 'freezes', or 'hangs,' it no longer accepts any input, whether from the keyboard or the mouse. Occasionally, a frozen application will return to normal: the problem may have been related to (say) a disk write command that did not execute, resulting in an time out, but with control retuned to the user. Applications which freeze may also crash the operating system, especially of a PC. However, the latest release of Windows® (the Millennium Edition) resolves this problem. Freezes followed by the need to re-boot and the possible loss of all current data are becoming less common.

Friode

A FRIed diode.

Full Monty / Monte

Anorak's PC fully loaded with every possible option and accessory, many of which will now be obsolete but 'cannot be thrown away'. Typically such a machine will run dual processors, and, amongst other things, have: several hard disks, ZIP, JAZZ, DAT, CD, CDR, CDRW, DVD, LS120, and 'Super-Floppy' drives, bespoke Tower case, Touchscreen, 23' Monitor, IR/Wireless keyboard and mouse, voice control, surround sound system with super bass woofer, 32Mb Video card with PAL output to Videowall projector, graphics editing suite, mixer desk and graphic equaliser, flight yoke and weapons system, steering wheel and pedals, flatbed and hand-held scanners, at least two printers, videoconferencing, digitising pad, light pen, headset, Wireless networking, Digicam, Webcam, UPS, Backup generator, and more ports and connector slots than you could shake a stick at.

Functional Requirements Specification

A comprehensive document, detailing what is required of an installation to meet the business needs of users. Such a document can run to considerable length and would normally be prepared by Analysts, who can speak the language of both business and IT; effectively, they act as interpreters between technical and non-technical areas.
As a basic principle, developments within commercial enterprises should be user-driven. The first step is to devise a Functional Specification, also known as the

Functional Requirements Specification, (FRS). This leads naturally to the Technical Specification and then, if necessary, to a Request For Proposal (RFP).

Future Proof

A term often used by system sales persons, who claim, almost incredibly, that their product will not become technologically outdated - at least not for the next few weeks!

Games

A Game is an item of entertainment software that provides enjoyment for the user but does not benefit the Organisation. It can be ill-advised to allow games onto an organisation system, especially those which allow a number of players to take part simultaneously through network connections. Networks have been brought almost to a halt by the sheer volume of traffic generated by staff playing games such as MUD (the Multi-User Dungeon game) and DOOM.
There are exceptions. Some 'games' have a useful training element and can be used to simulate real situations, for example Air Traffic Control simulations have been used to gauge users' ability to handle multiple variables and make decisions under pressure. Others have been designed specifically for training or assessment of abilities in business-specific situations, such as a Dealing Game for prospective Foreign Exchange traders.
Organisation policy should state the organisation's position regarding game software. Policy-makers would be well advised to restrict the use of games software to specific machines, not connected to the main system, for example computers in the Training Centre or in a staff recreation area.

Geek

Alternative term for an Anorak. Geeks are not normally malevolent, but their unquenchable desire to fiddle with pieces of equipment or software can lead to considerable trouble.

Ghost

An identity that does not relate to a real person. It is not unknown for staff with the necessary IT skills to create a fictitious user with a password which allows that user to access the system with impunity, knowing that an audit trail will lead nowhere. Ghosts may also appear on the payroll, courtesy of a user who has the power to create new files in the personnel and payroll systems.
The creation of user profiles and the granting of logical access rights is a high security function and must be strictly monitored, preferably with dual controls for creation and authorisation.

Gopher

A popular distributed document retrieval system which started at the university of Minnesota. Many hosts on the Internet now run Gopher servers which provide a menu of documents. A document may be a plain text file, sound, image, submenu, or other Gopher object. It may be stored on another host or may provide the ability to search through certain files for a given string.
Gopher has largely been superseded by the World Wide Web, a similar document retrieval system which includes access to Gopher documents.

Grass Line

Slang term for the telephone hotline operated by FAST -the Federation Against Software Theft. FAST exists to try and eradicate the illegal/unlicensed use of proprietary software and operates an informer service which can be used to provide information about companies or individuals. Several companies have been surprised to find that they have been reported and subsequently. Depending upon the circumstances and severity of the case, informers can claim rewards amounting to several thousand pounds.
Companies must ensure that ALL software used on their systems is properly licensed.

Guest

An occasional user of system who does not have a personal/ unique user ID and password but logs on infrequently as 'Guest'. This practice is quite common in offices where staff usually work in other locations and only log on as guests to the main system when in the base office. Guest passwords may also be granted to persons temporarily associated with the organisation, such as short term temporary staff, students, trainees, etc.
Since they are often not specific to a named individual, Guest passwords should normally allow only minimal access rights. 'Guests' are also commonly known as 'Visitors'.

Hacker

An individual whose primary aim in life is to penetrate the security defences of large, sophisticated, computer systems. A truly skilled hacker can penetrate a system right to the core, and withdraw again, without leaving a trace of the activity. Fortunately such individuals are relatively rare, (although the numbers are growing), and the majority of those persons which the media are prone to call Hackers are really only Anoraks, Geeks, etc., or possibly Proto-Hackers who can penetrate some systems and leave childish messages to prove how smart they are. Proto-Hackers are those who aspire to Hackerdom but have not yet acquired the necessary skills to get past serious security measures without setting off alarm systems.
Hackers, of whatever variety, are a threat to all computer systems which allow access from outside the organisation's premises, and the fact that most 'Hacking'

is just an intellectual challenge should not allow it to be dismissed as a prank. Clumsy hacking can do extensive damage to systems even when such damage was not intentional.
Statistics suggest that the world's primary Hacker target - the Pentagon - is attacked, on average, once every three minutes. How many of those attacks are from Hackers and how many from Government Agencies, criminals, and terrorists, around the world is another question entirely.....
The term is also applied (possibly unfairly) to those individuals who do not attack or attempt to penetrate computer systems, but use their skill to Hack commercially available packages, usually game software, to give themselves some advantage, make the game harder or different, etc. Such Hacks are often published in computer magazines as 'Hints, Tips, and Cheats' - much to the annoyance of the developers. This type of Hacker is not normally a threat to organisation computer systems except, possibly those of game software development companies.

Handshake

An electronic exchange of signals between pieces of equipment (fax machines, computers, computers and printers, etc.,) to establish that each has the necessary protocols installed to allow communication between the units; sometimes, also to confirm identities so that transmissions are routed to the correct destination.
An extension of the normal confirmation routine is the Challenge Handshake that is a demand for proof of identity and authorisation.

Harassment

The UK Protection from Harassment Act 1997 makes provision for protecting people from harassment and 'similar conduct'. It states that a person must not carry out actions which amount to harassment, or which they know may be regarded by the other person as harassment.
Claimants of harassment may be awarded damages for any anxiety caused by the harassment. An additional offence relates to putting the fear of violence on a person
In terms of Information Security, harassment by e-mail or via chat rooms may be punishable under this law.

Hard Copy

A copy on paper, as opposed to any other storage medium. Hard Copy is what falls out of computer printers in disturbing quantities.

Hardware

Physical equipment:- processors, screens, keyboards, mice, printers, scanners, network routers, hubs, bridges, racking, disk drives, portable drives, etc.
If you can kick it, it's hardware!

Hardware Inventory

Master Hardware Inventory - A detailed list of all hardware owned by the organisation, showing, amongst other things:- type, make, model, specifications, cost, location, user(s), and asset reference number.
Unit Hardware Inventory - an equally detailed list of hardware in order of user (individual or department). This sheet may be used for Audit checks to confirm that any given user still has the equipment detailed and no unauthorised additions, removals, or modifications have been made.

Hardware Platform

The term 'platform' refers to the hardware and operating system architecture, in which an application runs.

Health and Safety

Compliance with Health and Safety regulations is mandatory in most countries. In relation to Information Security, compliance is beneficial to security as the working environment and the precautions taken help reduce risks.

Help Desk

Staff, either within the organisation IT Department or based at a hardware/software supplier, who are responsible for assisting non-technical staff in the use of computer systems, and resolving problems which may arise. Staffing a Help Desk is an ulcerous job and many Help Desks perform superbly, but... The telephone lines of external Help Desks are frequently engaged and if/when contact is finally made, users will discover that many Help Desk staff are undoubted experts in negotiating the very small print contained in contracts and warranty agreements. (See also Hose and Close).

HEX / Hexadecimal

Hexadecimal, or 'Hex' for short is a numbering system using base 16 (as opposed to the usual base 10). Hex is a useful way to express binary computer numbers in which a byte is normally expressed as having 8 bits; with 2 hex characters representing eight binary digits – aka a byte.
'Hex' is word, sometimes used by 'techies' to throw ordinary users off the scent; invariably it only clouds the issue!

Hex Editor

Hex editors are commonly available 'tools' (or utilities) which allow the user to scrutinise **and update** the precise contents of the hard disk. Not only do they reveal the hexadecimal equivalent of the binary code in which the data is stored,

but they also helpfully provide an ASCII converter which allows you to make sense of the contents. All fine so far. However, because they permit searches and updates, it is possible, indeed easy, to search for an expected string / word, and then update that string with a new value (e.g. by substituting the value '5644' for '9480'). Because the number of bytes has remained the same, the data file in which this string is found, may not have been corrupted, however the integrity of the data has been destroyed, and the subsequent user of the file may have little evidence of such tapering.
In addition, a hex editor is able to reveal data believed to be safe within password protected files, or even data in files which have been deleted but have yet to be overwritten.
The use of checksums can confirm that a file has not been tampered with, even slightly. However, more fundamentally, Security Officers should endeavour to prevent hex editors from being loaded onto any of the organisation's PCs / workstations in the first place.

Hose and Close

An off-putting practice of some Technical Support / Help Desk staff. In response to a question from a distressed user, Support responds with a deluge of technobabble which the user doesn't understand, issues a series of abstruse command instructions, which the user cannot follow, and then hangs up before the user can come back with a request for a simple explanation.
The tech support staff can mark another tick on the 'support provided' sheet, but the user is not only no further forward, but may also have been charged a premium rates per minute – just to be made to feel foolish.
Happily, there are a growing number of Tech Support hotlines which do communicate in plain language.

Host

A large computer, running major applications and containing considerable quantities of data which is contacted through a network by subordinate computers (PCs, terminals, etc) for processing or information. Smaller hosts are generally known as servers.

Hot Desking

A relatively new approach to working whereby staff do not have their own, dedicated facilities, but share them with other workers – i.e. there are fewer desks and computers than there are staff.
Two kinds of situation are common :-

1. Call centres and similar functions which run 24x7 on shifts. As one staff member logs off and leaves, another takes over, logging on with a new ID and password.
2. 'Field' staff such as sales representatives check in to base to complete paperwork, upload/download files, etc.. Such staff will use any desk/computer that happens to be free.

In either case, password control systems and audit trails are essential to monitor which user is doing what, with which machine.

Hot Standby

A contingency/fallback approach to maintaining system availability whereby a second system, with the same configuration as the main system is kept running - often 'mirroring' the processing of the main system - ready to take over the processing load instantaneously, should there be any failure in the main system.

Housekeeping

Routine care of a computer system to ensure that it is kept running in the most efficient manner. Housekeeping will normally include: routines to delete items such as temporary files (which are no longer required), identify and remove duplicates of files, check the integrity of the disk records and the magnetic coatings on the disk surfaces, and generally tidy up the filing system.
Housekeeping should not be restricted to the main system. It is just as useful for desktop machines and laptops - considering the circumstances under which they are used!

HTTP

This protocol, the Hyper Text Transfer Protocol, is used for the transmission of information, graphics, sounds and animation between a client Web browser and the Web server.

HTTPS and SSL

The Secure Hyper Text Transfer Protocol uses HTTP but additionally activates Web server security, in the form of Secure Sockets Layer (SSL). This means that the communications between the client and the (host) Web server are encrypted and, additionally, that the host Web server may be validated by the client using a Digital Certificate on the server.
The URL for such Web sites indicates that they are secure by the use of 'https://address' (rather than http://address), and it also features the yellow padlock in the browser's status bar.

Identity Hacking

Posting on the Internet or Bulletin Board(s) anonymously, pseudonymously, or giving a completely false name/address/telephone with intent to deceive. This is a controversial activity, generating much discussion amongst those who maintain the net sites. There are two cases in which problems can be caused for organisations:-

1. a member of staff engages in such practices and is 'found out' by net users, thereby associating the organisation name with the activity.

2. a posting by an unrelated third party, pretending to be the organisation, or a representative.

In either case, if such posts are abusive, or otherwise intended to stir up an argument, the likely result is a Flame Attack, or Mail Bombing.

Impact Analysis

As part of an Information Security Risk Assessment, you should identify the threats to your Business Assets and the impact such threats could have, if the threat resulted in a genuine incident.
Such analysis should quantify the value of the Business Assets being protected to decide on the appropriate level of safeguards.

Incursion

A penetration of the system by an unauthorised source. Similar to an Intrusion, the primary difference is that Incursions are classed as 'Hostile'.

Information Asset

An Information Asset is a definable piece of information, stored in any manner which is recognised as 'valuable' to the organisation. The information which comprises an Information Asset, may be little more than a prospect name and address file; or it may be the plans for the release of the latest in a range of products to compete with competitors.
Irrespective, the nature of the information assets themselves, they all have one or more of the following characteristics :-

- They are recognised to be of value to the organisation.
- They are not easily replaceable without cost, skill, time, resources or a combination.
- They form a part of the organisation's corporate identity, without which, the organisation may be threatened.
- Their Data Classification would normally be Proprietary, Highly Confidential or even Top Secret.

It is the purpose of Information Security to identify the threats against, the risks and the associated potential damage to, and the safeguarding of Information Assets.

Information Custodian

An Information Custodian is the person responsible for overseeing and implementing the necessary safeguards to protect the information assets, at the level classified by the Information Owner.
This could be the System Administrator, controlling access to a computer network; or a specific application program or even a standard filing cabinet.

Information Owner

The person who creates, or initiates the creation or storage of the information, is the initial owner. In an organisation, possibly with divisions, departments and sections, the owner becomes the unit itself with the person responsible, being the designated 'head' of that unit.
The Information Owner is responsible for ensuring that :-

- An agreed classification hierarchy is agreed and that this is appropriate for the types of information processed for that business / unit.
- Classify all information stored into the agreed types and create an inventory (listing) of each type.
- For each document or file within each of the classification categories, append its agreed (confidentiality) classification. Its availability should be determined by the respective classification.
- Ensure that, for each classification type, the appropriate level of information security safeguards are available e.g. the logon controls and access permissions applied by the Information Custodian provide the required levels of confidentiality.
- Periodically, check to ensure that information continues to be classified appropriately and that the safeguards remain valid and operative.

Information Security Guidelines

An Information Security Guidelines is a suggested action or recommendation to address an area of the Information Security Policy. A security guideline is not a mandatory action, and no disciplinary action should result from non adoption. However, Information Security Guidelines are considered Best Practice and should be implemented whenever possible.
A guideline typically uses works like "should" or "may" in the definition. Guidelines are usually written for a particular environment and are used to help guide users' actions. For example, "all successful logins **should** be logged and monitored." A guideline may apply to management, administrators, end users, or a specific group within the organisation.
Information Security Guidelines will usually supplement the Procedures Manuals with their adoption encouraged and promoted rather than enforced.

Information Security Incident

An Information Security incident is an event which appears to be a breach of the organisation's Information Security safeguards. It is important to respond calmly and to follow a logical procedure, first to prevent the breach from continuing, if possible, and second, to inform the appropriate person(s) within the organisation; this usually includes the appointed Security Officer.

N.B. Where a member of staff fails to observe Information Security procedures; this is not, of itself, an Information Security incident. However, depending

on the risk of the incident, disciplinary and/or improved procedures may be required.

Information Security Plan

The Information Security plan complements the IT Plan in so far as it documents, budgets and resources the upgrades to both hardware, software, training and procedures, in relation to Information Security.
The driving force behind the Information Security Plan will be the Security Officer with the executive sponsor likely to be the Chief Information Officer, or the Chief Executive Officer / Managing Director.

Information Security Policy

Information Security Policy is an organisational document usually ratified by senior management and distributed throughout an organisation to anyone with access rights to the organisation's IT systems and / or information resources.
The Information Security Policy aims to reduce the risk of, and minimise the effect (or cost) of, security incidents. It establishes the ground rules under which the organisation should operate its information systems. The formation of the Information Security Policy will be driven by many factors, a key one of which is **risk**. How much risk is the organisation willing and able to take?
The individual Information Security Policies should each be observed by personnel and contractors alike. Some policies will be observed only by persons with a specific job function, e.g. the System Administrator; other Policies will be complied with by all members of staff.
Compliance with the organisation's Information Security Policy should be a incorporated with both the Terms and Conditions of Employment and also their Job Description.

Information Security Risk Assessment

An Information Security Risk Assessment is an initiative which identifies :-

1. the nature and value of the Information Assets or Business Assets
2. the threats against those assets, both internal and external
3. the likelihood of those threats occurring
4. the impact upon the organisation.

Risk is defined as a danger, possibility of loss or injury; and the degree of probability of such loss. Before introducing Information Security safeguards, you must be aware of the dangers to which you are exposed, the risks and likelihood of such events taking place, and the estimated impact upon your organisation were each to actually occur.
In order to determine the overall level of Information Security safeguards required, you should consider performing a comprehensive Information Security Risk Assessment.

Information Systems

The computer systems and information sources used by an organisation to support its day to day operations.

Information User

An Information User is the person responsible for viewing / amending / updating the content of the information assets. This can be any user of the information in the inventory created by the Information Owner.

Information Warfare / Infowar

Also Cyberwar and Netwar. Infowar is the use of information and information systems as weapons in a conflict in which the information and information systems themselves are the targets.
Infowar has been divided into three classes;-

1. Individual Privacy
2. Industrial and Economic Espionage
3. Global information warfare, i.e. Nation State versus Nation State.

Most organisations will not need to be concerned over classes I and III, but clearly Class II is relevant to any organisation wishing to protect its confidential information.

Input

Describes, literally, (as a verb) the activity of 'putting in', or (as a noun) the material which has been put in, but, of course, being an IT expression, it has to be shortened and reversed.
Input may be manual or automatic, but in both cases the organisation system should have a means of checking the integrity of the material being entered and the authority of the originator to perform this function.

Interface

Interfaces facilitate communication between different computer systems or allow people to communicate with machines (and vice versa). Interfaces can be software, such as the Graphical User Interface (GUI) of Microsoft Windows®, or hardware, e.g. the physical connections between, say, a simple terminal and a host computer. Interfaces use an agreed protocol ('language') to send and receive information from one machine to another.

International Organization for Standardization – ISO

The International Organization for Standardization is a group of standards bodies from approximately 130 countries whose aim is to establish, promote and manage standards to facilitating the international exchange of goods and services.
The term 'ISO' is not an acronym for the IOS, it is a word derived from the Greek word 'isos' which means 'equal', which is the root of the prefix 'iso-'. For example the word isobar links together areas of equal atmospheric pressure.
In Information Security the ISO standard 17799 has recently been established. Based upon the British Standard – BS 7799.

Internet

A publicly accessible Wide Area Network that can be employed for communication between computers.
To many users, the terms: 'Internet' ('The Net') and 'World Wide Web' ('The Web') are synonymous. In fact, the Web - the best known part of the Net by virtue of all those www.name.com advertisements - is only one part of The Internet, which also includes: Usenet, Arpanet, Bulletin Boards, On-Line services, and a variety of other accessible networks.

Internet Service Provider – ISP

An Internet Service Provider – commonly referred to as an 'ISP', is a company which provides individuals and organisations with access to the Internet, plus a range of standard services such as e-mail and the hosting (running) of personal and corporate Web sites.
The larger ISPs will offer a range of access methods including telephone, leased line, ISDN or the newer DSL (ADSL) circuits and will be connected to 'backbone' high speed digital circuits which form the Internet itself.
ISPs usually charge a tariff for their services although income can be derived from various sources of advertising and portal activities.
Occasionally an ISP are referred to as IAP - an Internet Access provider.

Intervention

Human input in response to a request by the system while it is 'on hold'.
Interventions can be expected or unexpected, for example, providing a higher level password for authorisation, or responding to an error message indicating a fault, e.g. 'Printer Error: cannot print to LPT3, user intervention required'.
A log of unexpected interventions should be maintained and reviewed at intervals to check if a pattern is developing with a particular program, user, or piece of equipment, which may require some repair, fix, or other corrective action.

Intranet

A Local Area Network within an organisation, which is designed to look like, and work in the same way as, the Internet. Intranets are essentially private networks, and are not accessible to the public.

Intrusion

The IT equivalent of trespassing. An uninvited and unwelcome entry into a system by an unauthorised source. While Incursions are always seen as Hostile, Intrusions may well be innocent, having occurred in error.
Strong ID and password systems can minimise intrusions.

Intrusion Detection System IDS

Intrusion Detection Systems are complex software applications, which monitor network activity using various techniques, such as 'intelligent agents'. Many current applications will not only detect misuse but also identify a known pattern of attack, or attack scenario. The IDS can then automatically terminate the offending session and send an alert to the Systems Administrator.

IP Address

The IP Address or 'Internet Protocol' is the numeric address that guides all Internet traffic, such as e-mail and Web traffic, to its destination. The IP address is 'under the hood' and is derived from its domain name, which is mapped to the IP Address through the Domain Name Service.

Iron Box

A special environment set up to trap an intruder, logging in over remote connections for long enough to be traced. May include a modified shell, restricting the intruder's movements in unobvious ways, and 'bait' files, designed to keep the intruder interested and logged on.

ISDN

Integrated Services Digital Network. Provides for point to point data transmission at 128K bps. ISDN users must connect to a host, which is also capable of ISDN connection using an adaptor. The reliability of ISDN is not questioned, however, it is relatively expensive and is being eclipsed by the recent growth in broadband Digital Subscriber line technology.

IT Plan

An IT Plan is the means of executing your IT Strategy. Typically, it comprises the regular replacement of old hardware, upgrading of software and features, and the support and contribution to known Business Systems Projects.

IT Strategy

An IT Strategy sets out projected hardware and software development. It outlines the current, 'as is' hardware and software platforms (environments), and envisages how that environment will change over time - the future, 'to be' environment.
For an IT Strategy to be of benefit, its implications need to be conveyed to organisation staff so all can appreciate how it will affect their work in the future.

Java / Java Script

Java is an applications programming language which was developed by SUN Microsystems in 1995. Similar in look and feel to C++, Java was designed for the distributed environment of the Internet. It is based upon object orientation, and the resultant code is portable; which means that Java applications can run on many operating systems, not just the system which compiled it.
Java Script is an interpreted scripting language; similar in capability to Microsoft's Visual Basic or SUN Microsystems' Perl scripting language. Java script is interpreted, not compiled, and therefore slower to execute than compiled code; but it is easier to maintain and fast enough for small applications.

Job (IT Operations)

A series of tasks, or units or work, which a computer performs, the sum total of which may be described as a job. For example printing reports from many individual systems may be called 'the print job'.

JOOTT

Pronounced 'Jute'; it stands for 'Just One Of Those Things'. Sooner or later every organisation/user will run into problems which are not amenable to logical or technical solutions, or even plain common sense. JOOTT is used to describe those inexplicable computer problems which fix themselves, or are fixed by turning off the machine and restarting, or in more persistent cases, reinstalling the software. Nobody knows what caused the problem, or why it went away, it was JOOTT!

Key Disk

1. A copy protection device more usually associated with games than business software. One Key Disk is supplied with the original software.

Unless the disk is inserted into the Floppy Diskette Drive A: the program will not run.

2. A diskette required to enable a PC to start up. Some companies have adopted a personal key disk policy, whereby each user must insert their own Key Disk into a PC Floppy Drive A: before they can start up the PC. This approach does not relieve the need for an ID and password, but adds another layer of physical and logical security, because an unauthorised user cannot start the machine to attempt a log on.

   Key Disks often use non-standard formats, and frequently contain hidden, immovable files to defeat standard disk-copying methods. Users therefore cannot normally copy these disks, and loss, corruption, or failure of the disk can only be corrected by in-house technical staff.

KISS

1. Keep It Simple, Stupid
2. Keep It Short and Simple

Laptop

Laptop has become a generic expression for all portable computers. The earliest were described by some users as 'luggables' but as the size and weight of such equipment fell (and still continues to do so), the names have changed from luggable, to portable, Laptop, Notebook, Sub-Notebook, and Palmtop.
Laptops are more expensive than desktops and require extra security measures, if only because of their obvious attractiveness to thieves.

LCD

Liquid Crystal Display

LED

Light-Emitting Diode A Diode which emits light, <gasp>. Does exactly what it says on the 'tin'.

Legacy / Heritage System

A legacy system is a hardware and software system which uses technologies which are 'old' in comparison with today's technology. Typically, legacy systems use character terminals (although many have been made to look smarter by enabling access through a Graphical User Interface), and process data through a proprietary database etc.

Legacy Tech

Techie term for hardware and/or software which is basically obsolete, but cannot yet be disposed of, either because of the size of investment expended to obtain it in the first place, or because the cost of replacement by upgrade or migration is beyond the resources of the organisation. The continued use of such technology often means that the organisation cannot take advantage of advances in software capabilities, since new programs will not run with their old hardware or operating systems.
There are large numbers of Legacy systems still in use at all levels, from old IBM installations down to networks running applications, written in a now-defunct programming language. Some, such as PCs still running DOS or Windows® 3.1 systems, can be dealt with on a piecemeal basis, while others will require a complete and simultaneous cutover. Organisation management would do well to identify all such systems, and establish a prioritised programme for replacement, as resources permit.

Library

An area of the computer which retains software files in an orderly and secure manner.

Live / Production

When a system is 'in production' or is said to be 'live', it means that it is being used to process active work or transactions, and it is no longer in test mode. Organisations should always differentiate between and separate systems which are being evaluated, tested, or developed from those which are 'live'.

Load / Systems Loading

The 'load' on a system refers to the demands placed upon it. The overall load combines many factors and includes :-

- Total storage capacity for programs and data
- Number of applications being run concurrently
- Number of concurrent users, peaks, troughs and average
- Number of peripherals: e.g. using a file server as a print server increases demand, as each printed document is 'spooled' to the server's disk before being queued to the printer.

Whilst the sizing of hardware can become complex, once the above points are clear, other factors, such as expected response times / performance can be considered.

Local Area Network

A private communications network owned and operated by a single organisation within one location. This may comprise one or more adjacent buildings, but a local network will normally be connected by fixed cables or, more recently, short range radio equipment. A LAN will not use modems or telephone lines for internal communications, although it may well include such equipment to allow selected users to connect to the external environment.

Locking

A technique used to prevent unauthorised changes to file contents, also known as 'Read Only'. Typically a document - for example a disciplinary letter to a member of staff, - will be created and then 'locked' with a password. Other authorised users will be able to view the contents and even make copies, but only the originator of the document has the password needed to gain access to change the content.

Lockout

Technique used to stop an (apparently) unauthorised attempt to gain access to the system. A typical example is the three tries limit on password entry. It may be a simple matter of a genuine user forgetting their ID and password, or making a mistake in trying to enter, but after three attempts, the system will Lockout that user and report an attempted intrusion to the Security Administrator. Information Security will have to reset the user records to allow another logon attempt.

Logging

The process of recording events at the time that they occur.

Loggon / off

The processes by which users start and stop using a computer system.

Logic bomb

Also known as Slag Code and commonly associated with Disgruntled Employee Syndrome, a Logic Bomb is a piece of program code buried within another program, designed to perform some malicious act. Such devices tend to be the province of technical staff (non-technical staff rarely have the access rights and even more rarely the programming skills required) and operate in two ways:-

1. '**Triggered Event**' for example, the program will review the payroll records each day to ensure that the programmer responsible is still

employed. If the programmers name is suddenly removed (by virtue of having been fired) the Logic Bomb will activate another piece of code to Slag (destroy) vital files on the organisation's system. Smarter programmers will build in a suitable delay between these two events (say 2-3 months) so that investigators do not immediately recognise cause and effect.

2. '**Still Here**' - in these case the programmer buries coding similar to the Triggered Event type but in this instance the program will run unless it is deactivated by the programmer (effectively telling the program - "I am still here - do not run") at regular intervals, typically once each quarter. If the programmer's employment is terminated unexpectedly, the program will not be deactivated and will attack the system at the next due date. This type of Logic Bomb is much more dangerous, since it will run even if the programmer is only temporarily absent - eg through sickness, injury or other unforeseen circumstances - at the deactivation point, and the fact that it wasn't meant to happen just then is of little comfort to organisation with a slagged system.

Logic Bombs demonstrate clearly the critical need for audit trails of activity on the system as well as strict segregation of duties and access rights between those staff who create systems - analysts, developers, programmers, - and the operations staff who actually run the system on a day-to-day basis.

Logical Access

Logical access refers to the connection of one device or system to another through the use of software. The software may run, say as the result of a user powering a PC, which then executes the login sequence, or it may be the result of internal processing between systems.

Logical Security

Software safeguards of the organisation's systems, for instance: IDs, Passwords, Access Rights, Authority levels, etc.

Luser

Contraction of the words 'Loser' and 'User'. A Luser is a member of staff with an uncanny ability to make a mess of the computer system quite innocently and without malice.
The type of individual who can really mess things up so badly that the damage is either irrecoverable, or the only hope is to restore from backup, is a 'Power Luser'. IT department fault logs should be used to identify any such individuals, and appropriate training or transfer to another function should be arranged at the earliest opportunity!

m-

Another abbreviated prefix which will soon be overused, standing for 'mobile'. It is being used to describe messaging and transactional activities which can be conducted using a mobile telephone, including access to E-mail, the Internet, and other communications. The term is often associated with WAP, and growing numbers of mobile telephones are being marketed as 'WAP enabled'; m-functions raise the combined security concerns of e-functions and laptops.
m-commerce, m-banking, m-dealing, - the list will grow.

Macro

A series of commands grouped together as a single command to automate repetitive and/or complex tasks. Technical purists argue as to whether or not writing macros is actually programming, but from the perspective of most end users, it amounts to pretty much the same thing. Macro recording facilities are now built in to most standard business/office software packages, covering word processing, spreadsheets, databases, graphics and presentations, etc.
Malicious macros are not unknown; they can be transmitted to other users through the document in which the macro is embedded. Whether or not creating a macro is regarded by an organisation as 'programming', it is advisable that all macros created or used within an organisation are checked for their function and compliance with security regulations.

Macro-Virus

A virus containing a malevolent macro. Depending upon the way the virus is delivered it may sometimes be known as a Trojan, or a Worm. The Melissa virus, is one of the best known macro viruses and infects the document template upon which hundreds (or thousands) of documents are based. Estimates vary, but damages of approximately $100 million may have resulted from the Melissa virus.

Magic Smoke

A substance trapped inside integrated circuit packages that enables them to function. Also known as 'blue smoke' it is similar to the archaic 'phlogiston' hypothesis about combustion. Its existence is proven by what happens when a chip burns up: the magic smoke gets out, so the computer doesn't work any more. QED.

Mainframe

Used originally as a term for almost any computer system, then to describe a large system, the term 'mainframe' is used less frequently as the numbers in use decline. This is due largely to the massive increase in processor power of smaller computers. A year 2000 home user desktop computer has more storage capacity and raw processing power than a 1966 vintage mainframe, and an entire

organisation can now be run with just one desktop server connected to a number of PCs.
Mainframes (and Supercomputers) are still being built, installed and run, but their use tends to be restricted to the scientific/academic/government communities rather than the commercial world.

Malicious Code

Malicious code includes all and any programs (including macros and scripts) which are deliberately coded in order to cause an unexpected (and usually, unwanted) event on a user's PC. However, whereas anti virus definitions ('vaccines') are released weekly or monthly, they operate retrospectively. In other words, someone's PC has to become infected with the virus before the anti-virus definition can be developed. In May 2000, when the 'Love Bug' was discovered, although the Anti Virus vendors worked around the clock, the virus had already infected tens of thousands of organisations around the world, before the vaccine became available. However, this may not be fast enough to prevent **your** PC from becoming infected with a virus that was delivered to your PC whilst you were innocently browsing a new Web site.
In June 2000 it was further revealed that a new type of attack was possible; called the 'No-Click' Stealth Bomb Attack. Such attacks use HTML, the code used for Web sites and, within this code, the pay load is then executed. The threat is that HTML is not only found on Web sites but can also be used to format and present the text of an e-mail. **This means that simply opening an e-mail encoded in HTML, could deliver its pay load with no user intervention at all**.
The solution is to run **both** a top rate anti-virus program and also a malicious code detection system which is able to constantly monitor the behaviour of downloaded "content" (e.g. a "harmless" page from a Web site) including executable files (.exe), scripts, ActiveX and Java. Such solutions can either run on individual PCs and workstations or from a central server.
See Compressors and Packers

Manhole

Alternative name for a developer's Back Door.

Masquerading

Identifying yourself as someone else, i.e. purporting to be another (probably genuine) user for example, sending an e-mail to a client under someone else's name. E-mail systems usually do not allow the sender's 'From' field to be altered, but those that do thereby permit messages to be sent under a completely false name.

Massaging Data

Especially when interfacing systems, it is often necessary to re-format or manipulate data from one format into another, to enable another system to accept the input, e.g. order processing output being input into the accounting system. Sometimes, the data will need to be massaged, e.g. by the removal of extraneous characters or the addition of some control characters. Whatever the exact requirements, such manipulation of data poses a threat to the integrity of the data, and thorough System Testing is advised.

Media

The physical material which stores computer information. Comes in two basic types - Fixed and Removable - and a variety of flavours:-
Hard Disk, Floppy Disk, Compact Disc, Laser Disk, Magneto-Optical Disk, Zip Disk, Super Floppy, Magnetic Tape Reel, Magnetic Tape Cartridge, Digital Audio Tape, Paper Tape, and so on and so forth.
Each of these have their 'for' and 'against' lobby groups, and there are no 'best' media, only the 'most appropriate' for a given organisation in given circumstances. Irrespective of which media are used, they will contain important data, and therefore must be used and stored under properly controlled conditions.

Methodology

A term that is often misused / misapplied. In systems development, the tasks required to achieve the end result can be complex and usually require adoption of a disciplined and formal approach. Having perfected such an approach, consulting companies and software developers will refer to their methodology. Methodology suggests an almost scientific and objective approach, which, of course, is rarely the case.

MicroFiche

Before the days of electronic data storage, computer print out was stored physically. Micro-fiche was a means of storing (relatively) large quantities of printed text and images on film transparencies in a greatly reduced (physical) form. Microfiche readers are required to project and magnify the output onto a backlit display.

Migration

Changing from one computer system to a different one, entailing changes in software and the transfer of data from the old system to the new, possibly necessitating conversion of data from the old format into another for use on the new system. For example: switching from an NCR-based system to an IBM constitutes a migration, while simply moving to a larger, newer, NCR system would be an 'upgrade'.

Migrations are complex, and any organisation contemplating or conducting one would be well advised to appoint a dedicated Project Manager and team, to ensure its smooth implementation.

Mirroring

1. Writing duplicate data to more than one device (usually two hard disks), in order to protect against loss of data in the event of device failure. This technique may be implemented in either hardware (sharing a disk controller and cables) or in software. It is a common feature of RAID systems. When this technique is used with magnetic tape storage systems, it is usually called 'twinning'.

   A less expensive alternative, which only limits the amount of data loss (rather than eliminating the risk entirely), is to make regular backups from a single disk to magnetic tape.
2. An archive or web site which keeps a copy of some or all of the files at another site so as to make them available more quickly to local users and to reduce the load on the source site. Such mirroring is usually done for particular directories or files on a specific remote server, as opposed to a cache or proxy server which keeps copies of everything that has been requested through it.

Mission Critical

Derived from Military usage, the term is used to describe activities, processing, etc., which are deemed vital to the organisation's business success and, possibly, its very existence.
Some major applications are described ad being Mission Critical in the sense that, if the application fails, crashes, or is otherwise unavailable to the organisation, it will have a significant negative impact upon the business. Although the definition will vary from organisation to organisation, such applications include accounts/billing, customer balances, computer controlled machinery and production lines, JIT ordering, delivery scheduling, etc.

Mockingbird

A Special type of Trojan Horse virus program, a Mockingbird is software that intercepts communications (especially login transactions) between users and hosts, and provides system-like responses to the users while saving their responses (especially account IDs and passwords) for later transmission to, or collection by, a third party.

Modem

MOdulator **DEM**odulator. A piece of communications equipment, which enables a computer to send transmissions through normal telephone lines.

Moore's Law

'The amount of information storable on a given amount of silicon has roughly doubled every year since the technology was invented.' First uttered in 1964 by semiconductor engineer Gordon Moore, co-founder of Intel in 1968, this held until the late 1970s, at which point the doubling period slowed to 18 months, however, as at the New Millenium, Moore's Law is again true.

Mouse Potato

Computer-using version of a Couch Potato. Identified by highly developed wrist and index finger, and complete lack of any other muscles.

Multi-tasking

Doing more than one thing at a time - or so it would seem. Human beings can multi-task: breathing, walking, thinking, and chewing gum, all at the very same time - but single processor computers do not.
It may seem that, for example, when a user is printing a file and viewing Web pages on the Net, the computer is doing two things at once, but, in practice, it is handling bits of each job, one after the other, so quickly that it just looks as though they are being done at the same time. Purists maintain that true multi-tasking requires more than one processor.
As the two or more programs squabble for memory space or communication port access on a single processor machine - such as a PC – multi-tasking causes more hang-ups, freezing, and plain JOOTTs than any other factor.

Murphy's Law

Also 'Sod's Law'. The correct, original Murphy's Law reads: 'If there are two or more ways to do something, and one of those ways can result in a catastrophe, then someone will do it.' The term originated with Edward A. Murphy, Jr., who was one of the engineers on the rocket-sled experiments, undertaken by the US Air Force in 1949 to test human acceleration tolerances. One experiment involved a set of 16 accelerometers mounted to different parts of the subject's body. There were two ways each sensor could be glued to its mount, and somebody methodically affixed all 16 the wrong way around. Murphy then made the original form of his pronouncement, which the test subject quoted at a news conference a few days later. Within months 'Murphy's Law' had spread to various technical cultures connected to aerospace engineering. Before too many years had gone by variants had passed into the popular imagination, changing as they went. Most of these are variants on 'Anything that can go wrong, will.' which is sometimes referred to as Finagle's Law.

Native Format

The native format refers to the default format of a data file created by its associated software program. For example, Microsoft Excel® produces its output as '.xls' files by default; this is the native format of Excel. Microsoft Word® produces native files with a '.doc' extension. Whilst many programs are capable of supporting other formats, they each have their native format.

Nerds

Alternative name for Anoraks.

Netwar

Alternative term for Infowar.

Network

A configuration of communications equipment and communication links by network cabling or satellite, which enables computers and their terminals to be geographically separated, while still connected to each other.

Network Administrator

Individual(s) responsible for the availability of the Network is available, and controlling its use. For smaller installations, this function is often combined with that of System Administrator.

News Group

News Group. Part of Usenet. Although termed 'News Groups', most of them are anything but this. They exist, theoretically for groups of like-minded users to ask questions and swap information etc. Currently there are approximately 60,000 News Groups covering virtually any subject imaginable, with titles ranging from '3b.config' to 'zz.unity.netlink'. Regrettably, most News Groups have their share of contributors whose sole mission appears to be to hurl abuse and 'flame' others' points of view, and some are definitely '18' rated. Caution is advised.

Non Disclosure Agreement – NDA

A Non Disclosure Agreement (NDA) is a legally binding document which protects the confidentiality of ideas, designs, plans, concepts or other commercial material. Most often, NDA's are signed by vendors, contractors, consultants and other non-employees who may come into contact with such material.

Non-Repudiation

For e-Commerce and other electronic transactions, including ATMs (cash machines), all parties to a transaction must be confident that the transaction is secure; that the parties are who they say they are (authentication), and that the transaction is verified as final. Systems must ensure that a party cannot subsequently repudiate (reject) a transaction. To protect and ensure digital trust, the parties to such systems may employ Digital Signatures, which will not only validate the sender, but will also 'time stamp' the transaction, so it cannot be claimed subsequently that the transaction was not authorised or not valid etc.

Notwork

Whimsical description of a Network which is not currently available to users, i.e. Not Working !!

O'Toole's Corollary

'Murphy was an optimist'

Object Code

The machine code generated by a source code language processor, such as an assembler or compiler. A file of object code may be immediately executable or it may require linking with other object code files, e.g. libraries, to produce a complete executable program.

Operating System

Computer programs that are primarily or entirely concerned with controlling the computer and its associated hardware, rather than with processing work for users. Computers can operate without application software, but cannot run without an operating system.
Major manufacturers - IBM etc., - tend to use proprietary operating systems, but popular commercial operating systems include Unix, Windows® 95/98/NT/2000, MacOS®, OS/2®, Linux®, and DOS® variants.

Operating System Hardening

Hardening of operating systems is the first step towards safeguarding systems from intrusion. Workstations and servers typically arrive from the vendor, installed with a multitude of development tools and utilities, which, although beneficial to the new user, also provide potential back-door access to an organisation's systems.
Hardening of an operating system involves the removal of all non essential tools, utilities and other systems administration options, any of which could be used to

ease a hacker's path to your systems. Following this, the hardening process will ensure that all appropriate security features are activated and configured correctly. Again, 'out of the box' systems will likely be set up for ease of access with access to 'root' / Administrator account. Some vendors have now recognised that a market exists for pre-hardened systems; see Trusted Operating Systems.

Output

Literally, material which is put out by the computer, (as instructed by an application program) often onto paper, but, increasingly, to a screen, or storage device.

Out-Sourcing

Having some or all of an organisation's computer processing performed by a separate specialist organisation, such as a computer payroll bureau. This approach can generate savings in resource, but rarely operates in real time and carries a high risk of breach of confidentiality.

Overhead

Overhead refers to the load placed upon a computer or system. For example, if a system, which usually has 10 persons processing transactions needs to accommodate 50, the overhead on the system has increased. Likewise, encrypting and decrypting data will increase a system's overhead and reduce the resources available for other processes during the encrypt/decrypt cycle.
Take care not to increase the overheads on your systems without due consideration of the impact this may have. Your systems may well have adequate capacity to absorb the extra load; but there again, they may not, and this may affect your Information Security.

PABX / PBX

A Private Automated Branch Exchange. The telephone network used by organisations to allow a single access number to offer multiple lines to outside callers, and to allow internal staff to share a range of external lines. All such exchanges are now automated, and it is common to refer to them as a simple 'PBX'.

Package Software

Software that is provided 'as is' or, 'Off the Shelf' by a supplier, and which is almost certainly in use by a number of organisations and companies.
Unless your organisation is prepared to be a beta test guinea pig, commercial users would be well advised to steer clear of package software which is **not** is use in any other organisation, and with evidence of some track record.

Padded Cell

Where a sensible organisation puts lusers so they can't do any damage. A program that limits a luser to a carefully restricted subset of the capabilities of the host system, and which is not so much aimed at enforcing security as protecting others (and the luser) from the consequences of the luser's boundless energy and enthusiasm.

Parallel Processing

A computer which uses more than one processor, either to be able to perform more than one task at the same time or to improve processing speed by breaking down one larger task between different processors. Parallel processing is not quite the same as 'Multi-tasking' since, by definition, a single processor cannot do two things at once. It just seems that way to the user because the two things are handled one after the other so very quickly.
A typical organisation/business server will employ at least two and often four processors within the same machine. Although they may appear identical from the outside, dual processor (and better) systems are not aimed at the domestic, home user, market. Generally they demand specifically written application software and are not suitable for games/entertainment use. This feature alone makes them more attractive to companies.
Some very large systems can employ huge numbers of processors - hundreds or more - and, naturally are extremely powerful (approaching the SuperComputer class). Such systems are generally described as being 'Massively Parallel'.
Parallel processing has considerable advantages fro companies with Mission Critical applications - but it comes at a price.

Parallel Running

The period during which a new and existing system run side by side, using the same data, performing the same processes, and generating the same outputs to prove the suitability of the new system. Parallel Running can be the last phase of a User Acceptance Testing program, to be followed, hopefully, by formal acceptance, and Cutover.

Parkinson's Law of Data

'Data expands to fill the space available for storage.', i.e. buying more memory encourages the use of more memory-intensive techniques. It has been observed since the mid-1980s that the memory usage of evolving systems tends to double roughly once every 18 months. Fortunately, (per Moore's Law) memory density available for a constant price also tends to about double once every 18 months. Unfortunately, the laws of physics mean that the latter cannot continue indefinitely.

Password Management Package

A piece of software that is used to control password functions, often for several different application systems simultaneously.

Passwords – Choosing

The object when choosing a password, is to make it as difficult as possible for a hacker (or even a business colleague), to guess or 'work out' your password. This leaves the hacker with no alternative but to a) give up (which is what we want!) or b) initiate a 'brute-force' search, trying every possible combination of letters, numbers, and other characters. A search of this sort, even processed on a computer capable of generating and testing thousands of passwords per second, could require many years to complete. So, in general, passwords should be safe; but only if you select them carefully.

Using only the standard English alphabet and numerals, a non-case-sensitive password of 6-characters offers over 2 million possible combinations. In case-sensitive password applications 'a' is not the same as 'A', which doubles the number of available characters. Thus, making that same 6 character password case-sensitive, and allowing the shifted version of the numerical keys increases the number of combinations to approaching 140 million . Each additional character increases the number of combinations exponentially, and so a 7-character, case-sensitive password would offer over a billion combinations. A human user has virtually no chance of ever identifying a 6-character password which has been randomly generated and, obviously, even less chance of cracking a password of 8 or more characters.

What Not to Use

- Don't use your login name in **any** form e.g. 'as is', reversed, capitalized, doubled, etc.
- Don't use your first or last name in any form.
- Don't use your spouse or partner's name; or that of one of your children.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, your home or street name etc.
- Don't use a password of all digits, or all the same letter. This **significantly** decreases the search time for a hacker.
- Don't use a word contained in the dictionary (English or foreign language), spelling lists, or other lists of words.
- Don't ever use a password shorter than six characters.

What to Use

- Use a password with mixed-case alphabetic characters.
- Use a password with non alphabetic characters, e.g., digits or punctuation.
- Use a password that you are able to commit to memory; so you don't have to write it down.

- Use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Be aware of Dictionary-Based Off-Line Searches

Hackers will often use a dictionary of common passwords to 'jump start' the cracking of your password. Instead of using passwords like "kwPpr*Kv8naiszf" or "2AW~#6k" many people still use simple, easy to remember passwords such as *jackie1* or *PeterS*. So hackers don't bother with exhaustive searches for all combinations of random letters or characters, but use a rules-based password cracking program.
Therefore select a password that will be extremely hard to crack and change it periodically too!

Passwords – Use and Best Practice

A string of characters input by a system user to substantiate their identity, and/or authority, and/or access rights, to the computer system that they wish to use. Passwords are central to all computer systems - even sophisticated systems employing fingerprints, voice recognition, or retinal scans.
Even having chosen an 'impossible to guess' password, (See Passwords – Choosing) your management of the password will determine its effectiveness in safeguarding access to the system using your user ID and password. The following best practice guidelines should be observed.

- Passwords must **never** (**ever**) be written down. The moment they are committed to a paper or a document, discovery of that paper will invalidate other security measures. A potential hacker may also witness the removal of the paper as you innocently review your password list, and this will then offer a simple target; obtain the paper and not only will 'this' password be available, but possibly those to other systems and credit card PIN numbers and perhaps your bank account etc……..
- Passwords of key role holders - such as System and Network administrators - should be copied and held under dual control in a fire-resistant, secure location, to enable access to the system by an authorised person in the unavoidable absence of the password holder.
- Passwords must be changed at regular intervals, and should be chosen privately by the individual users; and although often issued initially by the IT people, the password must be changed immediately.
- Password changes must be forced if necessary by implementing an expiry period after which a user's password will not be accepted and the next attempt to log on by that user will result in a security flash to the system console.
- No sensible system would allow a 'user' to remain on-line for up to two weeks trying all possible combinations, and a lockout must be activated after a predetermined number of failed attempts or a fixed amount of time.

Patch

Similar to a 'Fix', a Patch is a temporary arrangement used to overcome software problems or glitches. A patch will normally be released as a 'quick fix' prior to the next formal release of the software. Patches are usually (but not always) available on-line from the vendor's Web site.
Caution. A patch will usually (but not always) be an incremental addition to an assumed software version, i.e. the patch will assume that the software already installed is version 'x'. It is critical that the patch is applied carefully and that the software version to which it applies, is confirmed. Naturally, no software update should be performed without first having adequately tested the update. See System Testing.

Path

In IT systems, the path refers to the location of a file or directory on that system. On PCs using MS DOS® or Windows® , the path is as follows :-

driveletter:\directoryname\sub-directoryname\filename.suffix

In Microsoft Windows®, the term 'directory' is called a 'folder'; it is the same thing though!
Unix systems are similar but use a modified syntax, as follows :-

/directory/subdirectory/filename

Payload

The 'active' element of a virus. Some payloads are extremely malevolent, others merely childish, while yet others appear to have no real payload at all, simply reproducing or attaching themselves to existing files all over the place and filling up hard disks with clutter.

Peer Review

Peer Review refers to the checking and review of work performed by one's peers (equals) in a working group. The term is frequently used in projects where systems development takes place. Both systems analysts and programmers will have their work checked by each other and this forms a critical aspect to the quality process. Peers can usually identify each other's errors quickly and easily and can result in elevated performance.

Penetration

Intrusion, Trespassing, Unauthorised entry into a system. Merely contacting system or using a key board to enter a password is not penetration, but gaining access to the contents of the data files by these or other means does constitute Penetration.
Penetration Testing, is the execution of a testing plan, the sole purpose of which, is to attempt to hack into a system using known tools and techniques.

Percussive Maintenance

Old military term used to describe an approach to hardware problems - 'If it won't work - hit it'.
IT hardware engineers have added - 'If that doesn't work, - use a bigger hammer'. Surprisingly there can be some value in this approach when, for example, loose connections are jarred back into place ! However, we do not advocate this approach and take no responsibility for loss or damage resulting from trials of this nature!

Peripherals

Pieces of hardware attached to a computer rather than built into the machine itself. The term includes Printers, Scanners, Hard Drive Units, Portable drives, and other items which can be plugged into a port.

Physical Security

Physical Protection Measures to safeguard the Organisation's systems. Including but not limited to restrictions on entry to premises, restrictions on entry to computer department and Tank, locking/disabling equipment, disconnection, fire-resistant and tamper-resistant storage facilities, anti-theft measures, anti-vandal measures, etc.

Pickling

Archiving a working model of obsolete computer technology so that a machine will be available to read old archive records which were created and stored using that machines' system. Reportedly, Apple Computers have pickled a shrink-wrapped Apple II machine so that it can read Apple II software (if necessary) in the future.

Ping

'Ping' stands for Packet Internet (or Inter-Network) Groper and is a packet (small message) sent to test the validity / availability of an IP address on a network. The technical term for 'ping' is the Internet Control Message Protocol. Maliciously sending large volumes of 'Pings' to cause difficulties for anyone else attempting to access that address is known as Smurfing .

PKI

Where encryption of data is required, perhaps between the organisation's internal networks and between clients and representatives, a means of generating and managing the encryption keys is required.

PKI, or Public Key Infrastructure, is the use and management of cryptographic keys - a public key and a private key - for the secure transmission and authentication of data across public networks.
Caution : Whilst the overall mechanisms and concepts are generally agreed, there are differences amongst vendors.
A public key infrastructure consists of:

- A Certification Authority (CA) that issues and assures the authenticity of Digital Certificates. A Digital Certificate will include the public key or other information about the public key.
- A Registration Authority (RA) that validates requests for the issuance of Digital Certificates. The Registration Authority will authorise the issuance of the keys to the requestor by the Certificate Authority.
- A certificate management system. This will be a software application developed and provided by the vendor of the PKI system.
- A directory where the certificates, together with their public keys are stored; usually confirming to the X.500 standards.

Plain Text

Also known as ASCII text. Words and figures in unencrypted, unformatted, readable form.

Platform

Usually, nothing whatsoever to do with railway trains or stations! The term platform crept into IT jargon in the early 1990s and is now an accepted term in the vernacular. It refers to the hardware and, by implication, the Operating System of a certain type of computer.

Policy

A policy may be defined as 'An agreed approach in theoretical form, which has been agreed to / ratified by, a governing body, and which defines direction and degrees of freedom for action.' In other words, a policy is the stated views of the senior management (or Board of Directors) on a given subject.

Polling

Checking the status of an input line, sensor, or memory location to see if a particular external event has been registered. Typically used on fax machines to retrieve information from a remote source, the user, will dial from one fax machine to another, then press the polling button to get information from the remote fax machine.

Polymorphic

Term used to describe a virus which changes itself each time it replicates in an attempt to hide from Anti-virus software. Nasty.

POTS

POTS – Plain Old Telephone Service. This acronym was born in the early 1990s when everything (it seemed) HAD to have an acronym. The term POTS was created by systems' professionals to clarify their documentation and diagrams when referring to networks and computer links which perhaps only used or required the use of, the plain old telephone system! It also implies the older non digital copper wiring which was 'OK' for voice but was poor for data at speeds beyond 4800bps.

Privilege

Privilege is the term used throughout most (if not all) applications and systems to denote the level of operator permission, or authority. Privilege can be established at the file or folder (directory) level and can allow (say) Read only access, but prevent changes. Privileges can also refer to the extent to which a user is permitted to enter and confirm transactions / information within the system. In many systems, the security features will offer the ability to implement dual control or automatic escalation to the next 'highest' level, to assist with Information Security compliance and best practice.
Privileges are established at 2 levels, firstly at the network level, where the level of privilege is established with respect to general access rights and permissions; secondly, at the application level where the user's job function and responsibility will determine the level of privilege required.
In general, a user of an organisation's systems should be offered no more than is necessary to perform the function required. See also Privileged User.

Privileged User

A User who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and Network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users.

Process

1. A process, in business terms, refers to a series of linked tasks, which together, result in a specified objective. One can identify the Sales process which could start with the identification of markets, through to prospecting, to making the sale and to the receipt of payment.

2. In computer terms, a process refers to one of dozens of programs which are running to keep the computer running. When you run a software program, a number of processes may be started. Take a look at the Windows Task Manager in Windows ® NT or 2000® and select the 'Processes' tab. You may be surprised to see the number of processes running, each with its own Process ID number so that the operating system can track each one.

Production System

A (computer) system is said to be in production, when it is in live, day to day operation. Systems which have been developed and tested are said to be 'migrated into production'.

Project Plan

A project plan is a plan which specifies, to an adequate level of detail, the precise nature of the project about to be undertaken, the resources required, the responsibilities of each party, the tasks to be performed and the dependencies and constraints upon the project. Project plans are **much** more than a list of tasks presented in the form of a 'GANTT' chart.

Protocol

A set of formal rules describing how to transmit data, especially across a network. Low level protocols define the electrical and physical standards to be observed, bit- and byte-ordering and the transmission and error detection and correction of the bit stream. High level protocols deal with the data formatting, including the syntax of messages, the terminal to computer dialogue, character sets, sequencing of messages etc.
Some examples of protocols are : TCP/IP, the protocol used on the internet to send and receive information; HTTP – used for Web page communications, is a subset of TCP/IP.

Proto-hacker

Individual who has risen above the tinkering Anorak level with aspirations to be a Hacker - but does not yet have the necessary skills to crack a major system. Can cause much damage by clumsy entry Hacking and blundering around the system corrupting files - albeit unintentionally. Proto-hackers may have marginally more technical skills than Anoraks but still display immaturity by leaving calling cards, messages, graphics, etc.. As a result most of them are identified and caught before they graduate to being full Hackers.

Proxy Server

A proxy server is a computer server which acts in the place of individual users when connecting to Web sites. The proxy server receives requests from individual workstations and PCs and then sends this request to the Internet. It then delivers the resultant information to the requesting PC on the network.
When used in conjunction with a firewall, a proxy server's identify (and its connected PCs) is completely masked or hidden from other users. This is the manner in which secure sites operate.

Quarantine

Defensive tactic employed against viruses. Anti-virus software can often detect viruses which it cannot repair automatically.. In such cases the simplest option is to delete the file, but better quality anti-virus programs offer the option to Quarantine the file. This involves removing the file from its current location, encrypting it, and locking it in the quarantine area, ie part of the disk which is not accessible by any application except the anti-virus program, and certain disk utility tools.
Once in quarantine the anti-virus utility programs may be able to open the file and examine the contents to allow a user to extract any useful information, or, if sufficiently skilled, to remove the virus and effect a manual repair of the file.

Read-Only

1. A disk, file, data, document etc., which can be viewed, possibly copied, but cannot be changed.
2. Items within a system, such as a ROM Chip, which the system can read from, but not write to.

Reality Check

1. The simplest kind of test of software; doing the equivalent of asking it 'what is 2 + 2' and seeing if you get '4'. The software equivalent of a smoke test.
2. The act of letting a real user try out prototype software.

Real-time

'Live', 'As it happens'. Real-time systems pass entries, update records, accounts, balances, etc., immediately new data is received and make that data available to users within the limitations of the system. Typically, the response from the system will be measured in milli-seconds. If a real-time system is failing to present its response to users adequately fast, it may well be indicative of other bottlenecks, such as a saturated network or other processes competing for processor priority. A real time system is assumed to need immediate access to processor power and will have its priority set accordingly.

Reconciliation

In the IT context Reconciliation is a vital part of Acceptance Testing and Parallel Running whereby the output from both the 'old' and 'new' systems is compared to ensure that the new system is operating correctly. Clearly, if the old system claims that 2+2=4, while the new system differs - there is a problem. Reconciliation goes beyond mere arithmetic and it is essential that all outputs be reconciled, to allow for known changes in the new system, and identify any unexpected results.
It is critical that this be completed before the new system is accepted.

Recovery

1. The process, enabled by utility programs and disk toolkits, of 'undeleting' or otherwise getting back files which have disappeared unexpectedly .
2. The process of recreating files which have disappeared, or become corrupted, from backup copies.

Regression Testing

Regression Testing is a process which tests a system once again to ensure that it still functions as expected / as per specification. The reason for this renewed testing activity is usually when a material change occurs to the system. For example; a new hardware platform; a major release of the operating system (e.g. Windows NT® to Windows 2000®). In addition, where say, the software vendor releases a new version of its database, a comprehension regression test plan needs to be developed and completed to ensure that the reports, screen, scripts, Remote Procedure Calls and User options, are all functioning as expected. Warning! the chances are, that they will not work completely as expected, and that you will need to modify / change certain aspects of your configuration.

N.B. Regression Testing must also test the revised software by simulating its operational environment to ensure that all systems and interfaces still operate as expected.

Regression Testing should be conducted as per any system testing as proceed according to a Test Plan. **If you do not perform Regression Testing, then your system could fail** upon upgrade.

Remote Store / Remote Data Store

An off-site location, i.e. some distance from the computer system, devoted to the storage of computer media, and in particular backup files. Storage of data files etc. in another department of the same building is not considered to be 'remote'.

Removable Storage

Computer storage media - such as disks, tapes, CDs etc., that can easily be removed from a computer and moved to another location or used in another computer.

Repair

A technically demanding technique used to undo the damage done to a file by virus infection and/or corruption. Most virus infections can be repaired automatically by an anti-virus program, but there are some, together with other types of (non-viral) data corruption which must be handled manually.
This approach requires a relatively high level of technical skills and the use of special software tools which should not be available to ordinary users.
The damaged files should be removed from the main system to a separately partitioned area while being repaired.
If the damage is severe or extensive, affecting a number of files, consideration my be given to recovering an earlier copy of the file from backup.

Request for Proposal – RFP

The Request for Proposal – or RFP, is the document produced by the project team of the organisation when determining the supplier and/or solution to a commercial need or requirement.
The project team should already have ascertained the types of solution which are appropriate and the vendors which compete in that space. The RFP is sent by the organisation to each of the primary vendors, with the intention that each vendor responds with a written proposal detailing how they will provide the solution, and the terms and conditions of such supply.
Typically, an RFP will comprise the following items :

Item	Description
• Covering letter	Introductory letter explaining what is expected and required, in particular, the date by which the response is required. Depending upon size and complexity, this period may extend from weeks to months.
• Introduction	An introductory paragraph, stating to purpose of the RFP, the date by which submissions should be made, the means by which submissions should be made (e.g. by fax to …; or by e-mail to … etc)

Item	Description
• Organisation Overview	To enable vendors to place their options for a solution into context, they need an overview of the organisation and its activities.
• Project Overview	The aims and objectives of the project, and the extent to which the vendor's solution is anticipated to contribute towards such objectives.
• Key Requirements and Constraints	It is critical to specify the key requirements and any constraints; e.g. if you require a solution to run on / integrate with, your Windows® NT system, then it should be specified along with any and all other requirements. **Caution** :Vendors will often telephone, or try to arrange a private meeting in an effort to glean further 'inside' information in order to ensure that their response is attractive. Ensure that all vendors are treated equally and that each is given the same requirements and expectations.
• Scope Limitations	Specify the precise boundaries of the solution in terms of location, people (numbers), organisational units, type of user and anything else which may be relevant.
• Vendor questionnaire	The RFP should always include a questionnaire which requires a response from the vendor to demonstrate how their solution will meet the stated requirements etc. All questions should encourage a response that is objective.
• Specific contractual or other requirements	Provide the vendors with any material contractual requirements which they should be aware of prior to their response to the RFP.
• Additional Information e.g. customer references, demonstrations etc	Specify the types of additional information that you expect to be provided.

N.B. It is extremely important that all vendors are treated equally and fairly and, as such, it is worth spending adequate time in order to plan for and prepare the RFP. Information provided to one vendor, as a result of (say) a one on one meeting, and not provided to other vendors, would be viewed as biased or uncompetitive and could result in difficulties, especially where you expect to use that vendor in the future. Therefore, if it is necessary to provide additional information, as a result of an enquiry from one vendor, supply this to all.

Resilience

Resilience refers to the ability of a computer, or system, to both withstand a range of load fluctuations and also to remain stable under continuous and / or adverse conditions.

Response / Response Time

Response time usually refers to a user's subjective assessment of a computers 'response' to their request. Such requests could be to logon to the network, or could be to receive the confirmation code following entry of a transaction. The response time of a system results from the interaction of multiple components and not simple the 'power' of the computer itself (although this helps!) There could be massive contention across the network, or there could be heavy processing taking place on resulting in little available 'CPU' time to deal with your request. One way of improving response time, is to increase the priority of the process which you are running. However, such techniques are **not** adviseable, unless you are the System Administrator and have a good understanding of the impact such re-prioritisation may have.

Retention and deletion of E-mail Correspondence

Simple e-mails carry no legal status at this time. Their use should therefore be limited to basic correspondence upon which no legal reliance is placed. At present, the law is still evolving with regard to e-mail, but current practice appears to be either to retain everything as a part of your organisation's activities, or retain nothing. In practice, organisations will wish to retain e-mails, as they nevertheless represent a record of genuine business correspondence, notwithstanding the fact that their validity in a court of law may be challenged.
However, the use of a Digital Signature is now legally enforceable in some countries, and any messages received using such signatures could be considered legally valid and hence enforceable. See Digital Signature for further information.

Reversion

The process of reverting to a previous version of software or hardware.

RGB

Red Green Blue. The three primary colours in computers. To an artist the primaries are Red Yellow, Blue, but to engineers of light, Yellow is replaced by Green.

RL

Real Life. The time-space continuum inhabited by ordinary users, ie those with interests outside PCs, screens, and keyboards.

Road Warrior

An 'outdoor' member of staff whose 'office' is a laptop and cellular telephone. Such persons, because of the nature of their working environment, and, to some extent the personality types associate with such work may well require a more than proportional share of the organisation's computer housekeeping time.

Root

Very much a 'techie' term and refers to the most privileged access possible on a Unix computer system. With 'root' access, one can create, delete (or corrupt !) anything on the system. The use of 'root' is normally highly restricted with Systems Operations and support staff using accounts with limited privilege.
See also Super User.

Root Directory

In a computer's filing system on the hard disk, the root directory is the directory (or 'folder') from which all other directories will be created. In Microsoft Windows® the root is denoted by the symbol '\' and in the world of Unix is shown by '/' (just to be different!)
In Unix the all powerful user of the system is also known as root which permits access and all privileges to the root directory and hence the entire filing system.

Rotation of Duties

Accompanied by Segregation of Duties, Rotation is a useful security measure which has, in the past, uncovered a number of users nefarious activities. In days gone by rotation was particularly important for staff such as cashiers in the habit of fiddling their till balances. Now it is aimed more at staff who use organisation computer systems. The logic behind the approach is that a new set of eyes on a situation may uncover irregularities - for example, the use of unauthorised, unlicensed, software.
Alternatively it may serve merely to prove that all is in order. Either way it is useful to know.

Routine

In IT, generally, a set of computer Commands/instructions forming part of a program. For ease and clarity of programming, software often consists of numerous modules, routines, sub-routines, etc., each of which can, if necessary, be programmed by a different person, only being brought together at the final stages.

RSA

RSA stands for Rivest, Shamir and Adleman, who are the developers of the public-key encryption and authentication algorithm. They also founders of RSA Data Security which is now RSA Security www.rsasecurity.com.
The capability to use RSA security is incorporated within the browsers of both Microsoft and Netscape and other major corporate communication tools such as Lotus Domino® / Notes®.
The creation, use and management of the Public and Private keys which are required for RSA security, use Public Key Infrastructure , or PKI.

RSI

Repetitive Strain Injury. Damage to limbs as result of overuse on mouse of keyboard. Typically 'Trigger Finger' suffered by a 'Mouse Potato'

Sacrificial Host

A computer server placed outside an organisation's Internet Firewall to provide a service that might otherwise compromise the local net's security.

Salami Slicing

A technique employed successfully by criminally inclined IT staff to acquire large sums of money, by means of very small amounts. Essentially it needs something like a Foreign Exchange business environment where there are large numbers of transactions involving more than 2 decimal places. As currencies, generally, only use two places decimals beyond this point are rounded off. Salami Slicing programs will always round down the amount, and transfer the additional places to a separate, hidden account which has a balance accumulating, over time, to a significant figure; multi-million dollar sums have been involved. This approach can only really work with systems handling huge numbers of transactions and where the amounts will not be noticed.
Very difficult to spot, and usually only comes to light (if at all) when the individuals involved leave the organisation, or are observed to be living well beyond their salary levels with no visible other means of support.

Sales Droid

Pejorative term for a computer sales representative.

Samurai

A hacker who hires out for legal cracking jobs, snooping for factions in corporate political fights, lawyers pursuing privacy-rights and First Amendment cases, and other parties with 'legitimate' reasons to need an electronic locksmith. Some have modelled themselves on the 'net cowboys' of William Gibson's cyberpunk SF novels. Some Samurai claim to adhere to a rigid ethic of loyalty to their employers and to disdain the vandalism and theft practiced by criminal crackers as beneath them and contrary to the hacker ethic. Some quote Miyamoto Musashi's 'Book of Five Rings', a classic of historical Samurai doctrine, in support of these principles.

Sanity Check

Checking a piece of work – IT related or anything else - for completely stupid mistakes. The term implies that the check is to make sure the author was sane when the work was produced. Often difficult to prove!

Scanning

1. Using a peripheral device to 'capture' documents, text, graphics, etc., into a system to make the information available to users.
2. Using a radio device to scan the airwaves for electronic transmissions with view to interception.

Scope Creep

Scope Creep is the expression used by project managers and/or vendors who are under pressure to constantly deliver in excess of what was originally agreed. Scope creep normally results from a failure to establish the clear requirements of the business users. As these begin to solidify the scope of the original plan can start to move – and continue to move. If the project manager is not alert to this (all too common) phenomenon, the requirements will constantly change thus ensuring that the projects spends years on delivering nothing, as they are continually reviewing and altering direction.
Scope Creep – do not allow it to happen to you!

Screamer

A VERY fast PC. Currently, to qualify as a 'Screamer' a PC must have **at least** a 1.5 Ghz processor and probably well in excess of a 30GB hard disk with a minimum of 256MB RAM; and as for the graphics card (oh, boy!).

Screen Capture

Formal term for Screen Grabbing.

Screen Grab

Taking a 'snapshot' of a computer screen to be used in a document. Most screen grabbing is legitimate and is a useful device for documents such as guides and instruction manuals where the reader can see exactly what is mean by the text, rather than trying to imagine it. Some screen grabs are less innocent and have been used to obtain information from files which can be displayed but not copied or printed.

Screen Savers

Screen savers, once created to save the screen from premature CRT burn out, are now used as a means of both protecting the screen and also for preventing casual shoulder surfing! Screen savers do have a useful and valid Information Security role. Used correctly, they will cut-in, blank the screen from view and require a user or network Administrator password to regain access. Provided the screen saver is set to trigger after (say) 2 minutes of inactivity, and upon user request, it can provide a useful and effective means of diverting casual / opportunistic incidents.

Screen Scraping

Screen scraping is a technique used to interface (or link together) one system with another, by means of emulating User (screen) interaction. Screen scraping 'maps' the location of the various screens and the input boxes (fields) for the information. Screen scraping will then emulate the input of an (electronic) User using the system at a terminal. This technique is not the preferred means of interfacing systems as it is slow and rather crude. However, it remains a viable means where other interfaces options are not easy or viable.

Screen Widow

'Significant Other' of a computer 'enthusiast'. Tech version of a grass widow.

Scripts

In a programming context Scripts are a type of programming language which are run, or executed, by another program. For example, Java Script is run by the Web browser which is running on the user's PC.
In the context of System Testing and User Acceptance Testing, scripts are used as the pre-determined input data to test the system. Scripts should not only state the precise data to be input, but also the expected response from the system. As User Acceptance Testing proceeds, the results from running the scripts will be recorded,

as will the overall system conditions at the time to allow developers to more easily debug errors.
Scripts can take the form of input data sheets for manual input, or can be a series of files, the processing of which simulates the generation of transactions across the network to the system. This latter approach can allow for significant volumes to be processed. However, it is **essential** to proceed carefully as errors can so easily compound making analysis a nightmare!

Second Site

A contingency arrangement whereby the organisation maintains a second computer centre, geographically remote from the primary system, but capable of taking over all processing and system functionality should the primary system fail.

Secure Area (on a system)

Where an unknown file – e.g. one downloaded from the Internet – is to be opened (and this is especially true for any executable file i.e. a .exe file (a program), it must ***not*** be opened or executed in the normal filing space for your live systems. A Secure Area – sometimes referred to as a 'Sand Pit' – is an area on a system which is totally shielded and / or isolated, from the potential impact of any code which is executed there. Whilst the isolation of the system is a clear requirement, scanning software which is able to detect malicious code activity must also be used, as Trojan code activity may go undetected.

Security Administrator

Individual(s) who are responsible for all security aspects of a system on a day-to-day basis. The security administrator should be independent of both development and operations staff and often holds the highest power password on the system in order than the most sensitive activities can only be undertaken with a combination of both System Administrator and Security Administrator top-level passwords.

Security Breach

A breach of security is where a stated organisational policy or legal requirement regarding Information Security, has been contravened. However every incident which suggests that the Confidentiality, Integrity and Availability of the information has been inappropriately changed, can be considered a Security Incident. Every Security Breach will always be initiated via a Security Incident, only if confirmed does it become a security breach.

Security for Electronic Transactions – SET

SET was originally supported by companies such as MasterCard, VISA, Microsoft and Netscape and provides a means for enabling secure transactions between purchaser, merchant (vendor) and bank. The system is based upon the use of a

electronic wallet which, carries details of the credit card, the owner and, critically a Digital Certificate. To provide end to end encryption and authentication, the SSL standard is used between the parties, thus ensuring digital trust between each leg of the transaction.

Security Incident

A security incident is an alert to the possibility that a breach of security may be taking, or may have taken, place.

Security Officer

The Security Officer in an organisation is the person who takes primary responsibility for the security related affairs of the organisation. It matters not whether the organisation is comprised two persons or two thousand, someone should be the named individual who becomes accountable for the Information Security of the organisation.

SED

Smoke Emitting Diode (from Light Emitting Diode). A component which has allowed the magic smoke to get out.

Segregation of Duties

A method of working whereby tasks are apportioned between different members of staff in order to reduce the scope for error and fraud. For example, users who create data are not permitted to authorise processing; Systems Development staff are not allowed to be involved with live operations.
This approach will not eliminate collusion between members of staff in different areas, but is a deterrent. In addition, the segregation of duties provides a safeguard to your staff and contractors against the possibility of unintentional damage through accident or incompetence – 'what they are not able to do (on the system) they cannot be blamed for'.

Serial Processing

Literally doing one thing after another. Generally Serial Processing is meant to indicate that one computer job must be completed before the next can begin and a queuing system is used, coupled with priority flags to indicate when a particular job request will be processed.
The most common example of serial processing is printing - especially when shared by several users.

Server

Typically a dual (or better) processor computer which supplies (serves) a network of less powerful machines such as desktop PCs, with applications, data, messaging, communications, information, etc.. The term is replacing 'host' in many situations since the processing power of a desk top server is such that one machine is sufficient to run the computing requirements of a complete organisation.

Service Level Agreement – SLA

A Service Level Agreement (SLA) is a contract between your organisation and the vendor of your system(s) to provide a range of support services, up to an agreed minimum standard. SLAs will usually specific precisely what the support procedures are to be and the way in which a support call will be escalated through the vendor's support organisation to achieve resolution.
SLAs should always have a maximum response time. In other words, from the moment the call is logged with the vendor, the SLA should specify the response time until either, an engineer arrives on site or perhaps a member of technical support calls back.
It is very important to discuss the details of the SLA with the vendor because, often, the only time when you will use it, is when you have suffered a breakdown or problem with your systems and it is then that you will need to depend upon the 'fine print' of the SLA.

Shareware

Software supplied on a 'try before you buy' basis. Shareware is produced by software companies and independent programmers and supplied to users through a variety of channels including magazine cover disks, e-mail, mail order, Internet downloads, etc. The basic idea is that users will try out the software (which is sometimes, but not always crippled or limited in some way) and will like it so much that they will pay a relatively small registration fee to become an authorised user of the unrestricted program.
Shareware has been very successful and several software houses have established themselves as niche market leaders this way but companies should exercise caution in the use of such material. Shareware form independent programmers has a reputation for being 'buggy', causing conflicts with other software already installed on the computer, or simply failing to perform as expected.
Companies with policies which permit the installation and use of such material should restrict it to stand alone test or development machines where the software behaviour and the programs claimed benefits can be examined fully before being installed as registered version on live machines.

Sheep Dip

Slang term for a computer which connects to a network only under strictly controlled conditions and is used for the purpose of running anti-virus checks on suspect files, incoming messages etc.

It may be inconvenient, and time-consuming, for a organisation to give all incoming E-mail attachment a 'health check' but the rapid spread of macro-viruses associated with word processor and spreadsheet documents, such as the 'Resume' virus circulating in May 2000, makes this approach worth while.

Shoulder Surfing

Looking over a user's shoulder as they enter a password. This is one of the easiest ways of obtaining a password to breach system security. The practice is not restricted to office computers, it is used wherever passwords, PINs, or other ID codes are used.
Could the person behind you at the bank ATM be a shoulder surfer?

Sign-Off

The term 'sign off', as used in the world of systems means an agreement, as evidenced by the customer's signature, that the system or project, meets the specified requirements. Much pressure will be brought to bear for users to sign-off on systems, or specific deliverables. Prior to sign-off, ensure that the system does indeed meet the requirements and / or projects milestones agreed.

Simulation

1. Simulation software - Sometimes classed as a game, but more often used in a business training or decision-making environment to replicate situations from real life but without the risk! For example an Air Traffic Control simulation allows controllers to hone their skills without the risk of a 'mid-air passenger exchange' or 'aluminium rain' Similarly, FX traders can deal without losing the organisation a real fortune, business managers/economists/regulators etc., can follow the effects of their decisions over a number of accounting periods in just a few hours. Good package simulations are relatively rare, and specifically written versions are expensive.
2. Exercises to simulate emergencies such as a major virus infection, or sudden loss of system (achieved quite simply by the expedient method of switching the system off!) can be extremely useful in monitoring organisation performance during the emergency as well as providing many hours of frustration and/or amusement for management and staff. For the organisation, it is never a good time to run such an exercise, but the lessons to be learned from such an exercise can prove invaluable should a real emergency ever arise.

Sizing

Sizing is an activity which is sometimes overlooked as today's systems are usually so 'powerful' that formal sizing appears pointless. A sizing exercise analyses the demands to be placed upon a system, in terms of concurrent users, data types and

quantity, storage requirements, expected response times etc and concludes the minimum specification for the system.

Slag

As a verb; - to run a destructive program which will render most or all of a computer systems files, records, and data, utterly useless.
As a noun; - a description of what is left of a computer system after the slag code has been run.
Normally associated with IT staff, and Logic Bombs, Slag Code has, allegedly, been used by a Hacker to destroy a computer system. Slag Code has also been used to blackmail organisations such banks into handing over significant sums in return for information as to the location of the code and deactivation procedures.
More recently, the term has acquired alternative meanings:-

1. To bring a network to its knees by overloading it with data traffic
2. To describe all the irrelevant and uninteresting material which has to be waded through on the Net while trying to reach the once piece of valuable information sought. This is also known as Bitslag.

Smart Card

Smart cards look, and feel like, credit cards, but have one important difference, they have a 'programmable' micro-chip embedded. Their uses are extremely varied but, for Information Security, the are often used, not only to authenticate the holder, but also to present the range of functions associated with that user's profile.
Smart Cards will often have an associated PIN number or password to provide a further safeguard. The main benefits of using Smart Cards is that their allocation can be strictly controlled, they are hard to forge and are required to be physically inserted into a 'reader' to initiate the authenticate process.

Smoke Emitting Diode

An incorrectly connected diode, probably an LED, in the process of losing its Magic Smoke and becoming a Friode.

Smoke Test

1. A rudimentary form of testing applied to electronic equipment following repair or reconfiguration, in which power is applied and the tester checks for sparks, smoke, or other dramatic signs of fundamental failure.
2. By extension, the first run of a piece of software after construction or a critical change.

Smurf / Smurfing

A smurf attack is one that is very technical and exploits features of the IP protocol within the TCP/IP protocol used for Internet communications.
A smurf attack causes a victim's computer to become completely 'way laid' with answering fictitious network requests ('Pings') that it grinds to a halt and prevents anyone else from logging on.
See Denial Of Service for further information.

Snail Mail

Bits of dead tree sent via the postal service as opposed to electronic mail. One's postal address is, correspondingly, a 'snail (mail) address'. The variant 'paper-net' is a hackish way of referring to the postal service, comparing it to a very slow, low-reliability network.

Sniffers

A sniffer is a program which captures and analyses packets of data as it passes across a network. They are used by network administrators who wish to analyse loading across network segments, especially where they suspect that spurious packets are 'bleeding' from one network to another.
The other use of sniffers is by connecting to the Internet then capturing data; such data can include user names and passwords. However, crackers who deploy sniffers usually target sniffers at a strategic position e.g. at the gateway between the target system and another network; through this gateway will pass all the login names and passwords. Having said that, most modern systems will ensure that the username and password is encrypted prior to transmission such that the sniffer will not yield such information 'on a plate'.

Social Engineering

Social engineering is a means by which information is extracted, usually verbally, by someone impersonating a legitimate holder or user of the information in question. Social engineering will often take place over the telephone; here are some examples :-

- A 'senior member of staff' calls the IT support desk in a 'great hurry' and has forgotten their password (and they need it now!)
- A 'secretary' calls to inform that their superior needs to access some information urgently but has forgotten the 'new' password.
- A 'telephone engineer' calls to request details of the access number to the computer system as they have received a fault log and they need to 'test it'.
- In response to a request from a 'colleague' to speak to Ms X, they are advised that she is away for 3 days on business. To the caller, this knowledge is indicative that Ms X's logon account to the system is unlikely to be used during this period.

Soft Copy

A document created and saved on computer media rather than paper. The transmission of 'soft copy' files between parties is now common place; especially since a de-facto standard has emerged for desktop tools such as Word Processor and Spread Sheet.

Softlifting

1. The piracy of software for individual use (as opposed to commercial piracy for gain).
2. The process of interrogating computers on a network, to gather intelligence on what software is being run on the machines. This can be a useful tool for security administrators to check compliance with software licences, and identify unauthorised or inappropriate activity.

Software Inventory

Master Software Inventory - A detailed list of all software licensed to the organisation, showing, amongst other things:- Licence number, program name, version/release number, cost, location(s), user(s), and asset reference number (if appropriate).
Unit Software Inventory - an equally detailed list of hardware in order of machine and user(s). This sheet may be used for Audit checks to confirm that any given user machine still has the software detailed and no unauthorised additions, removals, or modifications have been made.

Software Licensing

The use of unlicensed software is illegal, and whilst the majority of organisations would not condone it, the vast majority are believed to be using unlicensed software to some extent. In many cases, software piracy occurs unintentionally; for example a genuinely licensed program is copied for use on multiple workstations.
It is common practice for software vendors to permit customers to 'try before they buy'. In this case, they offer the software as 'shareware' and propose a trial of say, 30 days. At the expiration of the 30 day period, and depending upon the ingenuity of the developer, the software can refuse to load without the input of a valid licence key; or it can continue to run as normal or can require the continue depression of a button to signify your understanding of the terms of the licence.
Unlicensed software is major threat to an organisation's Information Security because, not only does this jeopardize the legal position, it also threatens the data held on such systems as no support will be provided.
The End User License Agreement – EULA is normally seen during the install process of the software.

Software Release

Since the early 1980s when the micro computer was (commercially) born, software packages have followed a standard release convention. A full release is a full digit, and a minor release is a decimal. For example Microsoft Windows® version 3.1. In general, the bigger the number, the longer the product has been used, and hence the more stable it is likely to be. This is not always the case and you should be cautious of new 'dot zero' releases, e.g. 2.0 as it could still be brand new code; and potentially untested.

Software Support / Maintenance Contract

Licences for business systems, especially the larger and more expensive ones, will usually be priced such that an annual support and maintenance agreement is incorporated, in additional to the software license agreement.
The price of such contracts will vary, but it is not unusual to see an annual figure of between 15% - 20% of the original software license fee. The support contract should offer a level of support in response to problems and issues, and specify precisely how such responses will be dealt with. Where such response is seen as critical to your organisation's business operation, you should consider a separate Service Level Agreement, in which specific metrics will be incorporated.
The 'maintenance' side of the agreement should specify the nature of such maintenance. For example it might specify that "clients will receive a minimum of two maintenance releases per annum which will include general software fixes together with general enhancements". To prevent expectation mismatch, it is suggested that you speak to a current customer of the system, who has some experience of the vendor's support and maintenance contract. Where this is not possible, seek tangible evidence of that which has been delivered over (say) the previous year.

Software Version Control

Although not a global standard per se, software developers have a generally agreed code of practice with regard to software versioning. In general, the version number will be identified by two or three digits e.g. (version) 1.2.1 This example indicates that the software is in its first **major** release, its second **point** release and its first mini release or **patch**.
Be wary of software in its '1.0' release as this suggests that the software is new and **may** not have undergone thorough testing and subsequent update. Be cautious when using any software in its 1.0 release; even those from the largest names in the software industry!

Source Code

The actual program - as written by the programmer - which is compiled into machine code (object code) which the computer can understand. Source code is the intellectual property of the developer(s) and for many years commercial source code was never released to users, only licensed for use. Possession of Source

Code is essential if a organisation is to maintain and/or modify the software without being reliant upon the original developer. There are now Escrow provisions in the agreements for major developments to protect users in the case of a developer/supplier ceasing to trade.

Spam

Derived from the Monty Python song 'Spam Spam Spam Spam', with seemingly endless repetition! Computer Spam is the electronic equivalent of Junk Mail. Companies and individuals who specialised previously in Mail Shots through the postal system have turned to Spam as a means of delivering (usually) worthless messages at a fraction of the cost of 'Snail Mail'. Given the huge databases now held on computers around the world, 'Spammers' can send literally hundreds of thousands of messages for a few pence, or cents. Some companies consider this to be a 'better' use of their marketing budgets than the traditional routes. Spam is also a feature of Usenet, where individuals, who need to get out more, post lengthy and irrelevant messages to dozens, if not hundreds, of groups at a time, attracting considerable irritation, generating significant amounts of angry message transmissions, and sometimes starting a Flame War.

Spoofing

1. Alternative term for Identity Hacking and Masquerading
2. The interception, alteration, and retransmission of data (in an attempt) to fool the recipient.

Spot Check

The term 'spot check' or 'snap check' comes from the need to validate compliance with procedures by performing impromptu checks on vouchers, records and other files which capture the organisation's day to day activities.

Stability

Because software can contain multiple bugs (or features!), a sought after characteristic is 'stability'. An operating system (e.g. Windows® NT or Sun Solaris) being described as stable, signifies that it may be used, as intended, without crashing, freezing or displaying other adverse characteristics.
Selecting an operating system for your primary systems, where reliability is essential, will require a stable environment. Hence the reason why most corporates will retain older versions of systems software to 'allow the bugs to be ironed out' before they migrate to the newer version. Even then, they will often consciously remain at least a 'point release' behind; valuing stability and reliability above all else.

Start of Day

Series of tasks, program loads, etc performed by IT department to make the system available for staff use at the beginning of the working day.

Stealth Bomb

A stealth bomb is a piece of malicious code that is disguised as something else. It may be received as a 'normal' e-mail, or perhaps as an amusing screen saver. Stealth bombs deliver their 'payload' surreptitiously and the results can be both damaging to your system and also highly embarrassing.
See Malicious Code for more detailed information.

Steganography

Steganography is the technique whereby a message, possibly encrypted, is concealed within another medium. In the world of computing, this means that a seemingly innocuous graphic or sound file (say) can conceal a message which could be used to disguise corporate espionage.

Stress Testing

Stress Testing is a form of testing which purposely attempts to identify the weakest link of a system. Stress testing will seek to verify that, following any abnormal conditions, the system can revert quickly to normal operation. Such conditions might include : data processing immediately after system downtime, after a network failure, or during peak activity periods.

Stripping

Deliberately deleting files, records, or data, from a system. This can be an authorised activity when, for example, duplicate files are identified and removed from the system to reclaim the disk storage space they occupy. More often, however, stripping is associated with the removal of records which evidence some fraudulent or other criminal activity. It is not unusual for Auditors, or Law Enforcement officers to find that the records they need for their investigations are not there.
Deleted records can be recovered if the storage media is secured quickly enough, but a skilled stripper can usually remove all trace of them before such action can be taken. The only recourse then is to backup files where (hopefully) copies can be obtained.

Structured Query Language – SQL

Structured Query Language or SQL (pronounced 'S' 'Q' 'L' or 'Seekwul') is a type of programming language used to interact with a database. The language is used to

both update and issue queries to the database. A query is a request for information based upon specific criteria e.g. 'output all our clients with a sales turnover of more than $x sorted by region'.

Suit

1 Ugly and uncomfortable 'business clothing' worn by non-hackers. Invariably worn with a 'tie', a strangulation device that partially cuts off the blood supply to the brain. It is thought that this explains much about the behaviour of suit-wearers.
2 A person who habitually wears suits, as distinct from a techie or hacker.

Suite

A collection of applications, each of which can stand alone, but which have been designed to work together. The most common example is the 'Office Suite' which will include, normally, a Word Processor, a Spreadsheet, a Presentation application, a Personal Organiser / Scheduler, probably an e-mail program, and, in some versions, a database application. The objective of the developer is clearly to try and lock in users to a particular set of programs rather than selecting separate appellations from different suppliers.

Super Computer

An extremely powerful, incredibly fast, and unbelievably expensive computer, such as the types associated with Cray, and up-scale IBM installations. Rarely seen in a business/commercial environment such machinery is usually the province of meteorologists, and research scientists.

Super User

The term 'Super User', is one that denoted the highest level of user privilege and can allow unlimited access to a system's file and set-up. Usually, Super User is the highest level of privilege for applications, as opposed to operating or network systems. Notwithstanding the possible semantics, the use of Super User should be under dual control as such a user could, if they so wished, destroy the organisation's systems maliciously or simply by accident; neither is acceptable!

Suppression

A technique used by criminals such as Salami Slicers to prevent particular records, accounts, etc being seen. Suppression code will stop a file being displayed on a screen, and will not include the item when a printed report is called. Very difficult to spot, especially since the total figure at the bottom of the report will be correct. The only way to prove that it is happening is to call for a list of all accounts, calculate, manually, the sum of the figures shown and compare that result with the claimed total. It is very unlikely that such a procedure would be carried out

unless there were already grounds for suspicion, but some Audit teams do follow such a practice for a random selection of ledgers, if only to justify their fee.

Surgery

1. The process of amending data or software through non-routine channels.
2. The area within IT department where file repairs etc., are carried out, and quite possibly the Sheep Dip machine is located.

SVGA

Super Video Graphics Array. Another type of screen. Better than VGA – which is hardly surprising – but not as good as XGA.

Sweeping

1. Automatically monitoring files to check if a particular event has taken place, for example an account balance has risen above, or fallen below a pre-determined figure.
2. Collecting data, or balances, from a list of files, or accounts, for consolidation purposes.

System Administrator

Individual(s) who are responsible for running/operating a system on a day-to-day basis. In smaller installations, this task may well include the Network Administrator functions, but should not include any Security administration responsibilities.

System of Record

A system of record is an information storage system (likely to be a computer system) which is the data source, for a given data element or piece information. The need to identify the Systems of Record can become acute in large organisations, where Management Information (or MIS) systems have been built by taking copies of output data from multiple (source) systems, re-processing the data and then re-presenting it for their own business uses.
Where the Integrity of the data (element) is vital, it must either be extracted directly from its System of Record or be linked directly to its System of Record. Where there is no direct link with the System of Record, the integrity, and hence validity, of the data is open to question.

System Requirements

A business, or other need, that must be satisfied by a computer system, and which therefore must be recognised when a system is being developed. Refer to Functional Requirement Specification.

System Software

System software is the general term used to describe the many software programs, drivers and utilities which, **together** enable a computer system to operate. One of the main components of system software is the operating system of the computer e.g. Microsoft Windows® 2000 Professional.

System Testing

The term System Testing can be used in a number of ways. In a general sense, the term 'system testing' refers to the testing of the system in artificial conditions to ensure that it should perform as expected and as required.

From a Systems Development perspective, System Testing refers to the testing performed by the development team (the programmers and other technicians) to ensure that the system works module by module ('unit testing') and also as a whole. System Testing should ensure that each function of the system works as expected and that any errors (bugs) are noted and analysed. It should additionally ensure that interfaces for export and import routines, function as required. System Testing does **not** concern itself with the functionality of the system and whether this is appropriate to meet the needs of the users. Having met the criteria of the Test Plan the software may then be passed for User Acceptance Testing.

Systems Development

Systems Development is the term used to describe the function of designing, coding, testing and updating software programs and other code e.g. scripts. The roles within Systems Development, will be Systems Analysts and Programmers and possibly other technical specialists.

Systems Operations

Systems Operations refers to a team, or possibly even a department within the IT group, which is responsible for the running of the centralised systems and networks.
Systems Operations personnel have 3 main types duty. Firstly they will run the day to day procedures for each of the main systems. Whilst these operations may well be automated, a systems operator will execute and oversee the operation. Secondly, they will perform routine housekeeping procedures on the systems, reviewing error logs and responding to any problems which occur day to day. Thirdly, Systems Operations personnel will run end of day and 'end of period' (e.g. monthly) procedures which will include the creation of backup copies of all the key data files across the systems.
From the above, it will be noted the Systems Operations do not concern themselves with development, testing or the functionality of the various software

applications being run. Their task is focussed upon maintaining maximum 'up-time' by keeping all system and networks running efficiently.

Talk Mode

Originally, a feature supported by some Operating Systems which allows two or more logged-in users to set up an on-line conversation in real time. Now, with the massive growth of the Internet, Chat, Newsgroups, and E-mail it has become much more common. Alternative names are Internet Relay Chat (IRC) Usenet Speak (US), and Espeak.. It combines the immediacy of talking with all the precision (and verbosity) that written language entails. It is difficult to communicate inflection, though conventions have arisen for some of these. Talk mode has a special set of jargon words, used to save typing, which are not used orally – except by some geriatric radio presenters. Some of these are identical to (and probably derived from) Morse-code jargon used by ham-radio amateurs since the 1920s.

TANJ

There Ain't No Justice (Larry Niven, Science Fiction author). Familiar cry of IT developers (when their new software doesn't work), and of users (when the software they've just bought hangs up their system and – as a bonus – requires the hard drive to be reformatted).

Tank

In larger installations, the area within the 'Computer Centre' in which the main computer systems are located. The term originates from the design of such rooms, which usually had half, or full, height glass windows on all sides, suggestive of life in a fish tank. Tanks are specially constructed rooms with complex environmental controls, because mainframe computers require low humidity and a relatively cool atmosphere. Access to 'the tank' is restricted to authorised personnel only, and usually have independent, clean line, uninterruptible power supplies, and extra (non-H2O) fire protection.
There are fewer Tanks to be seen now as newer servers do not require such critical climate control, but ALL systems irrespective of size, need reliable power supplies, and should be afforded proper fire protection.

TANSTAAFL

There Ain't No Such Thing As A Free Lunch (Robert A Heinlein, Science Fiction Author) The phrase owes some of its popularity to the high concentration of science-fiction fans and political libertarians in the IT world in general, and the hacking/programming fraternity in particular.

Tape Streamer

Peripheral Device used mainly for backing up data, which uses magnetic Tape rather than Disk.
Tape streamers are usually high capacity devices, capable of storing backups from more than one machine.

Techno Crime

Techno Crime is the term used by law enforcement agencies to denote criminal activity which uses (computer) technology, not as a tool to commit the crime, but as the subject of the crime itself. Techno Crime is usually pre-meditated and results in the deletion, corruption, alteration, theft or copying of data on an organisation's systems.
Techno Criminals will usually probe their prey system for weaknesses and will almost always leave an electronic 'calling card' to ensure that their pseudonym identity is known.

Techno Vandalism

Techno Vandalism is a term used to describe a hacker or cracker who breaks into a computer system with the sole intent of defacing and or destroying its contents. Techno Vandals can deploy 'sniffers' on the Internet to locate soft (insecure) targets and then execute a range of commands using a variety of protocols towards a range of ports. If this sounds complex - it is! The best weapon against such attacks is a firewall which will hide and disguise your organisation's presence on the Internet.

Terminal

Typically a Terminal will have only a screen and keyboard and can only operate by communicating with a host/server, having no processing power of its own. This type of terminal is often known as a 'Dumb Terminal' to differentiate it from PCs which are also used as terminals to communicate with a host, but can, and do, operate on a stand-alone basis without being connected to a host.
Terminals can have speed advantages over PCs since they work directly with the main system. For security conscious companies, dumb terminals are often a better choice than PCs. Users cannot introduce unauthorised software, or make 'inappropriate' use of the equipment since there are no facilities to do so. Most companies however, prefer the flexibility and power advantages that desktop PCs offer over terminals.

Terminal ID

The terminal ID is the identification number of a specific (physical) terminal or workstation on the network.

Test Plan

Tests on hardware and software must always be in accordance with a documented test plan. The key point about a test plan is that it not only documents what will be tested, but also the expected results. In addition, a test plan can identify additional areas which should be tested and the resultant plan more comprehensive.
Having completed the tests, the results need to be considered and a determination of whether or not, any results have failed to meet an acceptable standard. In particular, each failure should be allocated a 'severity level'. Without this gradation, an objective view cannot be taken. See also System Testing and User Acceptance Testing.

TFT

Thin Film Transistor. Type of Laptop Screen

Three Finger Salute

The keyboard combination that, under DOS, forces a warm (or soft) re-boot. On the great majority of PCs this is Ctrl+Alt+Delete but other machines may use other combinations. With Windows® 95 and beyond, Microsoft intercepted this command and presented some user options. However, if the PC is **really** hung, then continued three fingered salutes would normally cause a reboot. (Alternatively, most of us powered off or 're-set', at this stage). This was a favourite part of the PC user's day in the early 1990s when Microsoft Windows® 3.1 / 3.11 used to crash, freeze, and generally stop working, on a regular basis.

Three Strikes

Jocular reference to the security system of locking out users who fail to provide a valid password within three attempts - 'Three Strikes, You're Out !'

Time-bomb

As the name suggests, a piece of hidden program code designed to run at some time in the future, causing damage to, or loss of, the computer system. Time bombs are less sophisticated than Logic Bombs, being concerned only with the system date, rather than some specific event. Unless the date is changed, or the code removed, the Bomb will go off on a specific date, come what may.
A partial defence against such code is frequent backup of data. There is little to be gained by increasing the frequency of applications backup since the coded will be contained within these copies as well. Data from mission critical application should be backed up daily, if not actually mirrored in real time.

TLA

Three Letter Acronym

Tolerance

Alternative term for Resilience

Tool

A utility program used primarily to create, manipulate, modify, or analyse other programs, such as a compiler or an editor or a cross-referencing program, or perform maintenance and/or repairs on system hardware or application software. Tools include Hex editors, disk checkers, file backup and recovery programs, etc. Tools are powerful pieces of software and the use of tools within a organisation should be restricted to those personnel who have either received the proper training or have otherwise proven their competence in the use of such software.

Toolkit

A collection of tools with related purposes or functions, eg Anti-Virus Toolkit, Disk Toolkit, etc.

Total Cost of Ownership – TCO

The Total Cost of Ownership (TCO) is an annual cost representing the actual 'all in' cost of 'end user computing'. The issue has been pioneered by the respected business technology research company, Gartner Group Inc which currently estimates that a networked PC 'costs about $13,200 per node annually for hardware, software, support and administrative services and end-user operations'. Such costs are often greeted with disbelief; especially as the cost of the hardware continues to drop so appreciably. However, the material costs are found in 'end user operations' where the end users try to perform Systems Administration functions on their PCs or where they are simply trying to resolve a problem due to the ability to configure the operating system and desktop environments how they please. Many professionals in IT continue to rue the day when the computer became 'Personal'!
Managing TCO is consequently a substantial challenge to many large organisations.

Treeware

Less sardonic version of 'Dead Tree Edition'.

Trigger Finger

The index finger – used on mouse buttons, joysticks, weapons control systems, and the 'Reply to..' key of newsgroup postings.
Term used to describe injury/condition arising from over-use of said digit. Such a condition can disable a mouse potato completely.

Trojan

Term coined by hacker, turned spook, Dan Edwards. A Trojan Horse is a malicious, security-breaking program that is disguised as something benign, such as a directory lister, archiver, game or, in one notorious 1990 case on the Apple Macintosh, a program to search and destroy viruses! A Trojan is a type of virus which normally requires a user to perform some action before the payload can be activated. Famous examples include the recent (May 2000) attack by a virus known as 'Resume' in which an E-mail is received with an attachment which purports to be the CV of a lady seeking employment. A CV is actually attached, but embedded within it is a macro-virus which activates the Trojan program as soon as the document is opened for viewing. If the attachment is not opened, the virus cannot deliver the payload and no damage is done.
A basic defence against all viruses is a strict organisation policy that E-mail attachments should not be opened until they have been checked by an anti-virus scanner and then only if they originate from a known, reliable, source (even other known users may be infected). Any attachment which does not meet these criteria should be saved to a floppy disk and passed to your anti virus software vendor's investigation team to investigate. Meanwhile **the original E-mail message with its attachment must be deleted** from the user's system.

Troll

An E-mail message, Usenet posting, or other electronic communication, which is intentionally incorrect, but – unlike flame bait - not overtly controversial. Trolling aims to elicit an emotional reaction from those with a hair-trigger on the Reply To… key. A really subtle troll makes some people lose their minds. Not a good idea for organisation e-mail addresses to be associated with Trolls.

Trolling

Baiting readers on Usenet newsgroups with a post designed to incite a large volume of angry responses. Posts such as those that scream out racist epithets are common trolls. This activity is not normally a problem for companies - unless the person trolling happens to be using a organisation machine when the likely result may well be mail-bombing or other denial of service activity.

Trusted Operating Systems

Trusted Operating Systems are ones which have been specially modified to be so secure as to be almost unusable! They afford maximum security for those systems which require it …..
The reason for this development is due to the substantial rise in concern over the apparent ease by which hackers are able to gain access to seemingly **secure** systems, a number of vendors have developed variations on mainstream version of UNIX and Windows® which go well beyond the standard Operating System hardening which is advisable for all and any desktop and server systems.
However, the deployment of a trusted Operating system, does require substantially more training of your systems operations staff as, no longer does the Administrator necessarily have 'ultimate power'. Henceforth the functions which control say, file, print or network access, are now split into separate 'sandboxes' which permit only a subset of actions to be performed by one systems administrator. It will be apparent that a substantially higher degree of coordination is required with the Systems Operations team, and also a much deeper level of planning before any changes are made.
Whilst this may appear to be a high overhead; it does prevent a system from gradually being changed over time by a single Systems' Administrator making small changes 'here and there'. In effect the Operating System is locked down and such Trusted Systems lend themselves to any e-commerce business where maximum security is paramount; say e-banking.

Tunafish

Allegedly an age-old joke to be found in a computer manual, now advanced as a reason (or excuse) why something cannot be done, consisting of the line 'You can tune a file system, but you can't Tunafish'. Rumour has it that the joke was excised from later versions of the manual by humourless management droids.

Twip

Unit of measurement, One TWentIeth of a Point, ie 1/20 of a printer's point. There are thus 1,440 Twips to an inch or about 567 Twips to a centimetre. This unit of measurement seems only to have seen use in Billyware formats and products- notably Rich Text Format, Visual Basic, and Visual C++.

UK Data Protection Act

The Data Protection Act 1998 came into force on 1 March 2000 in the United Kingdom, and established rules for processing information of a personal nature and applies to paper records as well as those held on computers. The **Data Controller** is "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed". The principles of the Act are as follows :-

Anyone processing personal data must comply with the eight enforceable principles of good practice. Data must be:

1) fairly and lawfully processed
2) processed for limited purposes
3) adequate, relevant and not excessive
4) accurate
5) not kept longer than necessary
6) processed in accordance with the data subject's rights
7) secure
8) not transferred to countries without adequate protection

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply. With processing, the definition is far wider than before. For example, it incorporates the concepts of 'obtaining', holding' and 'disclosing'. For more information see http://wood.ccta.gov.uk/dpr/dpdoc.nsf .

UK Regulation of Investigatory Powers Act - RIPA

In February 2000, the UK Government introduced a Bill into Parliament called the Regulation of Investigatory Powers Bill RIPA).The aim of this Bill is to bring UK interception powers (and related issues) into line with the European Charter on Human Rights while updating UK interception powers to cope with technological developments such as the Internet.
In essence the RIPA will allow the law enforcement authorities to intercept any form of electronic communication and to acquire any electronic keys in order to decrypt the data. Note that such disclosure may require the holders of the data to breach confidentiality to such agencies.
This Act, which was given the Royal Assent in July 2000, remains controversial because :-

- it is unclear how it can conform to the European Charter on Human Rights.
- the surrender of a Digital Certificate to allow the authorities to decrypt the data (further) undermines Internet security and privacy in the UK.
- Internet Service Providers must maintain an 'interception capability' to enable the interception of e-mail and other traffic.
- it is likely to impose an additional cost on UK based Internet Service Providers; which will be passed on to both businesses and consumers.

Uninstall

1. To remove a program from a system completely. This is a more complex process than simply deleting the files in an obvious program directory, and is best achieved using an uninstaller which was active at the time of installation, to record ALL changes made to disk and file contents.
2. Euphemism for firing technical staff.

Uninterruptible Power Supplies - UPS

A UPS is a vital piece of hardware that should not be overlooked. Without it, a power 'outage' or even a surge, can shut down your systems within seconds. If this happens on a Windows® PC, the consequences are unlikely to be more than annoying and perhaps the loss of the work you were currently working on. However, if your server, running Windows® NT, 2000 or UNIX, suddenly has the power cut, the consequences can be more serious, as (potentially) hundreds of files can be left in an "open" state which, in the worst scenario, could prevent the system from rebooting properly – or even at all.
Therefore, the purchase and installation of a suitable sized UPS is vital. Because it contains its own battery(ies) it can not only prevent damage from sudden power surges, but it can continue to run your systems for between 15 minutes and 1 hour (or more), thus allowing an orderly, but speedy, close down.
However, a UPS is not supposed to allow the system to be operated for any length of time and, to provide a greater degree of protection against power cuts, a Backup Power Generator should be considered.

Up / Uptime

When systems arte said to be 'up' this means that they are running and (normally) accessible in the usual manner. Uptime, refers to the period during which the system is up. See Down and Downtime.

Upgrade

The process of replacing a version of software or hardware with a newer product release designed to meet new requirements, or generally improve performance. There may be no new requirements but a faster processor or later software release may generate efficiency savings, or introduce better security.

Upgrade path

According to sales personnel, this is the route by which the organisation's brand new computer installation is 'future proof'. It usually consists of a brochure full of pictures of bigger, faster, and more expensive machinery; **all** of which is likely to be obsolete by the time the organisation needs a new system !!

Upgrades

Upgrades should be the release of new software (or hardware) which genuinely fixes old problems and introduces new (and tested) functionality. Unfortunately, upgrades can become a clever means of charging customers for the functionality which they should have had when they first purchased the product! Normally, where a product has reported bugs and problems, the software vendor will release a patch.

URL

URL or Uniform Resource Locator is the techie term for the location of a file or resource on the Internet. The URL will always include the type of protocol being used e.g. http for a Web page or ftp for the address of a specific file which is to be downloaded.
An example URL using the http protocol is http://www.rusecure.co.uk/

Usenet

The part of the Internet populated by Newsgroups. The term 'news' is a little misleading since these groups are more in the nature of discussion groups. Usenet is relatively harmless, but access to newsgroups, as opposed to E-mail, is largely unnecessary for organisation users, except possibly for some of the groups dedicated to technical computer matters.

User Acceptance Testing – UAT

The test procedures that lead to formal 'acceptance' of new or changed systems. User Acceptance Testing is a critical phase of any 'systems' project and requires significant participation by the 'End Users'. To be of real use, an Acceptance Test Plan should be developed in order to plan precisely, and in detail, the means by which 'Acceptance' will be achieved. The final part of the UAT can also include a parallel run to prove the system against the current system.
The User Acceptance Test Plan will vary from system to system but, in general, the testing should be planned in order to provide a realistic and adequate exposure of the system to all reasonably expected events. The testing can be based upon the User Requirements Specification to which the system should conform.
As in any system though, problems will arise and it is important to have determined what will be the expected and required responses from the various parties concerned; including Users; Project Team; Vendors and possibly Consultants / Contractors.
In order to agree what such responses should be, the End Users and the Project Team need to develop and agree a range of 'Severity Levels'. These levels will range from (say) 1 to 6 and will **represent the relative severity, in terms of business / commercial impact, of a problem with the system, found during testing**. Here is an example which has been used successfully; '1' is the most severe; and '6' has the least impact :-

1. '**Show Stopper**' i.e. it is impossible to continue with the testing because of the severity of this error / bug
2. **Critical Problem**; testing can continue but we cannot go into production (live) with this problem
3. **Major Problem**; testing can continue but live this feature will cause severe disruption to business processes in live operation
4. **Medium Problem**; testing can continue and the system is likely to go live with only minimal departure from agreed business processes

5 **Minor Problem**; both testing and live operations may progress. This problem should be corrected, but little or no changes to business processes are envisaged

6 **'Cosmetic' Problem** e.g. colours; fonts; pitch size However, if such features are key to the business requirements they will warrant a higher severity level.

The users of the system, in consultation with the executive sponsor of the project, must then agree upon **the responsibilities** and **required actions** for each category of problem. For example, you may demand that **any** problems in severity level 1, receive priority response and that all testing will cease until such level 1 problems are resolved.

Caution. Even where the severity levels and the responses to each have been agreed by all parties; the allocation of a problem into its appropriate severity level can be subjective and open to question. To avoid the risk of lengthy and protracted exchanges over the categorisation of problems; we strongly advised that a range of examples are agreed in advance to ensure that there are no fundamental areas of disagreement; **or**, or if there are, these will be known in advance and your organisation is forewarned.

Finally, **it is crucial to agree the Criteria for Acceptance**. Because no system is entirely fault free, it must be agreed between End User and vendor, the maximum number of acceptable 'outstandings' in any particular category. Again, prior consideration of this is advisable.

N.B. In some cases, users may agree to accept ('sign off') the system subject to a range of conditions. These conditions need to be analysed as they may, perhaps unintentionally, seek additional functionality which could be classified as scope creep. In any event, any and all fixes from the software developers, must be subjected to rigorous System Testing and, where appropriate Regression Testing.

User Group (software application)

A User Group is often formed when a group of users of a common system believe that there is value in exchanging issues and solutions common amongst them. The User Group can also act as a common voice from the User Group to the vendor thus offering the possibility of consensus and focus where competing priorities could otherwise exist.

User Identity

A name, number, set of initials, etc., which, combined with a password, identifies, uniquely, a person authorised to use the system.

User IDs / User Name

User IDs are the backbone of most system's access security. The ID can be any combination of characters and is normally issued with a password. The (user) ID will usually remain fixed and is often the user's name or perhaps job title. Linked

to the ID will be a password which should be changed in accordance with your Information Security Policy.
The choice of User ID or User Name, is often selected by the Systems Administrator and will often be the user's name or initials; this is helpful for easy recognition of those logged into the system etc. However, having a User Name of 'StephenJI' is also reducing the effectiveness of one of the main security safeguards for all system's access; the User ID and password. If the User ID is already known, this allows a hacker to concentrate upon the password, in the certain knowledge that the User ID is correct!
However, be aware that many systems (especially PCs) will 'remember' the last User ID and will display it 'helpfully' (?!) upon login. You should consult your Systems Administrator, or other technical support person, to consider how to increase the effectiveness of the User ID and Password combination for the system in question.

User Interface

The User Interface is the way in which a system presents itself to, and interacts with, a human user. In today's Graphical Windowing environments the User Interface is a combination of the look, feel and overall logic of the 'man machine interface'.

User Requirements Specification – URS

The User Requirements Specification is a document produced by, or on behalf of your organisation, which documents the purposes for which a system is required – its functional requirements - usually in order of priority / gradation.
Whilst the URS will not usually probe the technical specification, it will nevertheless outline the expectations and, where essential may provide further detail e.g. the User Interface, say Microsoft Windows®, and the expected hardware platform etc.
The URS is an essential document which outlines precisely what the User (or customer) is expecting from this system. The term User Requirement Specification can also incorporate the functional requirements of the system or may be in a separate document labelled the Functional Requirements Specification – the FRS.

Users

The term 'User', whilst not being totally complimentary, (in the USA it suggests being a user of illegal drugs), means anyone who is using a system or computer. Users are not considered to be technically competent (otherwise they would be in IT!) and most problems are blamed on the users! In contrast, those who administer systems and networks would never consider themselves as users; despite the fact that they too have to write reports and use office programs like the rest of us!

Utility

A specialised program designed for more technical users as a tool, or set of tools, for checking the system, housekeeping, monitoring system health/status, repairing files, etc.
Access to utility programs by non-technical users should be restricted.

VDU

A VDU is a Visual Display Unit. Before computer displays became generally available with larger (17'+) monitors and high resolution graphs, the screen used to be referred to an 'the VDU'. Today, this term has been replaced by 'monitor'.

Vendor Support

Vendor support can be a major source of risk to Information Security. Although a system may meet functional requirements, if the vendor does not have adequate support arrangements e.g. an office within the same state, or even country, you should question this aspect most carefully. Vendors will always play down this aspect, for they wish to make the sale. However, your system and hence your information, is at risk if you are unable to obtain adequate support within a reasonable time frame.
Where a vendor does not maintain a support office within reasonable distance, an acceptable alternative is to arrange for priority telephone support. However, for this to work, it is often imperative that you maintain systems staff who are capable of diagnosing the issue and discussing the problem with the vendor's technical staff. In general users would not always be able to do this; not always because of their lack of technical knowledge about their system, but because they may also need knowledge of the operating system and the networking environment.
In general, maintaining a Service Level Agreement (SLA) with the vendor of your key operational systems is a necessary expense.

VESA

Video Electronics Standards Association

VGA

Video Graphics Array Another type of screen. Better than EGA, but (obviously) not as good as SVGA.

Virtual Private Network – VPN

A Virtual Private Network – or VPN, is a network which emulates a private network, although runs over public network lines and infrastructure. Using specialist

hardware and software, a VPN may be established running over the Internet. The use of encryption and a 'tunnelling protocol' maintains privacy.
Because public networks are used, the cost of a VPN costs a fraction of that of a traditional private network.

Virus

A virus is a form of malicious code and, as such it is potentially disruptive. It may also be transferred unknowingly from one computer to another. The term Virus includes all sort of variations on a theme, including the nastier variants of macro-viruses, Trojans, and Worms, but, for convenience, all such programs are classed simply as 'virus'.
Viruses are a very real problem for both organisation and individual computer users. At the present time there are very few, if any, virus which affect large computers, primarily because the programming languages which those systems use are not the same as those used to write virus code. Viruses, therefore are a problem primarily for users of PCs and servers.
As at April 2001, there were over 49,000 known viruses. Fortunately the great majority of these are classed as 'rare' and usually appear only in virus research centre files. However, that still leaves nearly 5,000 viruses, classed as 'common', roaming the world's computer networks, so there is absolutely no room for complacency.
They tend to fall into 3 groups:-
Dangerous; - such as 'Resume' and 'Loveletter' which do real, sometimes irrevocable, damage to a computer's system files, and the programs and data held on the computer's storage media, as well as attempting to steal and transmit user ID and password information
Childish; - such as 'Yeke', 'Hitchcock', 'Flip', and Diamond, which do not, generally, corrupt or destroy data, programs, or boot records, but restrict themselves to irritating activities such as displaying childish messages, playing sounds, flipping the screen upside down, or displaying animated graphics
Ineffective - those, such as 'Bleah', which appear to do nothing at all except reproduce themselves, or attach themselves to files in the system, thereby clogging up the storage media with unnecessary clutter. Some of these viruses are ineffective because of badly written code, - they should do something, but the virus writer didn't get it quite right.
Within all types there are some which operate on the basis of a 'triggered event' usually a date such as April 1st, or October 31st, or a time such 15:10 each day when the 'Tea Time' virus activates.
Organisations should maintain a 'virus diary' of known high risk dates/times to ensure that anti-virus measures are in place as required.

Visitor

Individual who is not a regular user of the system and has no registered/recognised ID or password.

Visitor Password

Generic password with extremely limited access rights used by Visitors .

Voice Mailbox

A mechanism whereby incoming telephone messages are recorded pending the availability of the intended recipient. Fancy IT version of the answer-phone.

Volume Testing

Volume Testing, as its name implies, is testing that purposely subjects a system (both hardware and software) to a series of tests where the volume of data being processed is the subject of the test. Such systems can be transactions processing systems capturing real time sales or could be database updates and or data retrieval.
Volume testing will seek to verify the physical and logical limits to a system's capacity and ascertain whether such limits are acceptable to meet the projected capacity of the organisation's business processing.

Vulcan Nerve Pinch

[from the old 'Star Trek' TV series via Commodore Amiga hackers] Alternative name for the Three Finger Salute

Web Site

An organisation's Web site is now as common as a Business Card but, unlike business cards, Web sites can offer anything from a simple 'electronic brochure', to an engaging experience of a product or service 'on line'. In just a few years, web sites have grown from being static and 'flat' pages, to those with animated 3-D graphics and sound and many pages are able to be built dynamically depending upon selections made.
The Web; it's what most people mean by 'the Internet'.

Webmaster

The person responsible for maintaining and updating the organisation's Web Site.

Webmistress

A lady Webmaster - obviously !

Weeding

Selective stripping of records, files, data, etc. More refined than 'stripping' which is more wholesale in nature, weeding can be as precise as removing one particular field from a database.

Well don't do it then

Standard help desk response to a Luser who complains that (for example) a particular combination of key strokes makes the PC do strange things. Derived from an old doctor's office joke about a patient with a trivial complaint.

Wetware

The human nervous system, as opposed to electronic computer hardware or software. Also, human beings (programmers, operators, administrators) associated with a computer system, as opposed to the system's hardware or software. Probably from the novels of Rudy Rucker, or, possibly, Stanislav Lem.

White Hat / Black Hat Hackers

Cyber terms. White Hat hackers are hackers who perform hacking for legitimate reasons; e.g. IT Security technicians testing their systems and researchers testing the limits of systems. On the other hand, Black Hat hackers are those who perform clandestine hacking for malicious reasons; such persons can also be referred to as 'crackers'. Grey Hat Hackers are those who seems to fall between both camps and Red Hat Linux® is a real problem to classify!

Wide Area Network

A communications network that extends beyond the organisation's immediate premises.

WINTEL

WINTEL is the short form of Windows® Intel® meaning an Intel processor based PC running a version of Microsoft Windows® e.g. 3.1, 95,98, NT or 2000. All these are forms of WINTEL PC. Of course, there are other microprocessor (chip) manufacturers who are making significant in roads into Intel's domination of the PC chip market. Hence the demise of the term WINTEL!

Workstation

The term workstation used to refer to extremely powerful desktop computers which were often (and still are) used by the scientific and research communities.

They tend to run the UNIX® operating system using powerful RISC processors with massive screens and superb graphics!
Today, however, whilst the above definition remains broadly true, workstation can also be used interchangeably with 'PC' where the computer is attached to the corporate network / LAN.

Worm

Classed as a type of virus. From 'Tapeworm' in the Science Fiction novel 'The Shockwave Rider' by John Brunner. A Worm is a malicious program that propagates itself over a network, reproducing itself as it goes.
The Anna Kournikova virus of March 2001, was written in the Visual Basic language with the code encrypted in an effort to disguise the contents. Additionally, the file was disguised as a graphic (.jpg) image of the famous tennis player. This Worm, and others like it, replicate themselves by generating outbound emails to all those persons listed in your e-mail address book.

WORM Disk

A 'Write Once Read Many' non-magnetic disk where, once data had been written to the disk, it could not be deleted, changed, or any more data added, but could be read, or copied to other media, as many times as required. Users of early CD drives used this technique to 'burn' programs and/or data onto a CD for distribution in the knowledge that it could not be altered in any way but was more reliable than removable magnetic media in situations where the disk would be accessed frequently.
Although advances in CD technology mean that in some cases more material can be added, and, most recently, can be deleted and the disk re-used, WORM disks are still the standard medium for distributing commercial software, and for companies distributing static data.

WWW

Verbal shorthand for the World Wide Web; the resources on networks (especially the Internet) which use the HTTP protocol to transmit data between client and server.

XGA

eXtended Graphics Array

XML

XML - eXtensible Markup Language is a markup language as is HTML for Web pages. However, whereas HTML describes data in terms of its display characteristics a page, XML describes data in terms of its content. In that respect

XML is a markup language that has significant potential for the capture and onward processing of data directly from Web pages.
The real significance of this is that Business to Business data transfer will be greatly facilitated by XML as neither party needs to write interfaces to each other's systems; they merely need to be able to accept and process XML.

YABA

Yet Another Blasted Acronym.

YATLA

Yet Another Three Letter Acronym.

YMMV

Your Mileage May Vary (standard excuse to cover things which don't behave the way the manual says they should)

Zip Disks

Zip® Disks, introduced by the Iomega corporation, have become a de-facto standard for transportable data storage. Being physically a little large than a 3.5' floppy disk, and yet able to store 250MB (or 100MB in older versions), makes the Zip® Disk an excellent choice for both transportable media and also security backups.
However, it is precisely **because** such large amounts of data may be easily copied and transported, that the use of such devices needs to be carefully controlled within the organisation. Please be aware that, only 10 years ago, 250MB was equivalent to the total storage capacity of most organisation's data, and whilst this may appear small by today's standards, it's capacity ensure that ensure client databases, product details, plans and charts etc, can be reliably copied onto a disk that fits into a shirt pocket.