Password policy

Overview

Purpose

This policy outlines the handling, responsibilities, and scope of passwords for the Information Technology (IT) resources of [Company Name]. This policy acts as an extension of the IT security policy for [Company Name].

Authority

This policy has full support from the [Company Name]'s executive steering committee and human resources department. The IT manager administers the policy, which is currently effective for all [Company Name] employees and computer systems.

Password policy

Mission

The IT objective of [Company Name] is to enable [Company Name] employees to perform their tasks with technology that is in good operating condition while appropriately addressing the business needs and keeping information secure within our IT resources.

The [Company Name] password dilemma

Passwords are the entry point to our IT resources. Protecting access to our resources is pivotal in ensuring that our systems remain secure. While we have not been exploited, nor do we expect to be, we must be diligent in guarding access to our resources and protecting them from threats both inside and outside our organization.

Password handling

Passwords for *all* systems are subject to the following rules:

- No passwords are to be spoken, written, e-mailed, hinted at, shared, or in any way known to anyone other than the user involved. This includes supervisors and personal assistants.
- No passwords are to be shared in order to "cover" for someone out of the office. Contact IT, and it will gladly create a temporary account if there are resources you need to access.
- Passwords are not to be your name, address, date of birth, username, nickname, or any term that could easily be guessed by someone who is familiar with you.
- Passwords are not be displayed or concealed on your workspace.

Systems involved

The [Company Name] password policy will address the passwords for the following IT systems with their rules:

- **Network and client operating system**: Windows 2000 username and password (Users will automatically be prompted at a login to change the password every 45 days.)
- **Outlook/Exchange groupware**: Windows 2000 username and password (Users will automatically be prompted at a login to change the password every 45 days.)
- **Computer BIOS password**: Hardware-level access to your computer (This password will not automatically change.)

- **VPN password**: The [Company Name] telecommuting system (Users will be prompted to change this password once a year.)
- **ERP system**: SAP credentials to the production system (Users will be prompted to change this password once a year.)
- **WWW accounts**: Credentials to external Web resources (These passwords are rarely changed unless initiated by the user. IT has disabled the option for these credentials to be saved [IE password caching] on all [Company Name] computers.)

Password composition

The following systems have systematically enforced password requirements as stated:

- **Network and client operating system (and Outlook)**: Passwords must meet the following criteria:
    - Password may not contain all or part of the user's account name.
    - Password is at least six characters long.
    - Password contains characters from three of the following four categories:
        - English uppercase characters (A…Z)
        - English lowercase characters (a…z)
        - Base 10 digits (0…9)
        - Nonalphanumeric (exclamation point [!], dollar sign [$], pound sign [#], percent sign [%], etc.)

Support

All [Company Name] users are to contact the IT staff for support of the password policy. IT welcomes your questions and suggestions and strives to keep our resources secure.

Administrative passwords

Administrative passwords are subject to stringent composition, frequent change, and limited access. This includes passwords for routers, switches, WAN links, firewalls, servers, Internet connections, administrative-level network operating system accounts, and any other IT resource.

Passwords for administrative resources must meet the following criteria:

- Password is at least 10 characters long.
- Password contains mixed case.
- Password contains at least three nonalphnumeric characters.
- Password contains at least two numbers.

Responsibilities

IT has the responsibility to enforce this policy. This can be done through systematic means and interaction with users.

[Company Name] users are responsible for complying with this policy.

Continuance

This policy is a living document and may be modified at any time by the IT manager, the executive steering committee, or the human resources department.

Summary

This policy is designed to secure [Company Name] resources. This enables [Company Name] to achieve its business objectives. Full cooperation with this policy is appreciated so that all goals can be met in accordance with the business objectives.

Disclaimer: This policy is not a substitute for legal advice. If you have legal questions related to this policy, see your lawyer.