Definitions

Application Administration Account: Any account that is for the administration of an application (i.e. SQL database administrator, etc.).

Password: A string of characters which serves as authentication of a person's identity, which may be used to grant or deny access to private or shared data.

Strong Password: A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically, the longer the password, the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about the password owner such as a birth date, social security number, and so on.

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of {COMPANY-NAME}'s entire corporate network. As such, all {COMPANY-NAME} employees or volunteers/directors (including contractors and vendors with access to {COMPANY-NAME} systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Audience

This policy applies to all personnel or volunteers/directors who have, or are responsible for, an account (or any form of access that supports or requires a password) on any system that resides at any {COMPANY-NAME} facility, has access to the {COMPANY-NAME} network, or stores any non-public {COMPANY-NAME} information.

Policy Detail

User Network Passwords

- Passwords for {COMPANY-NAME} network access must be implemented according to the following guidelines:
- Passwords must be changed every 90 days
- Passwords must adhere to a minimum length of 10 characters
- Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (!@#$%^&*_+=?/~’;’,<>|\).
- Passwords must not be easily tied back to the account owner such as:
- username, social security number, nickname, relative’s names, birth date, etc.
- Passwords must not be dictionary words or acronyms
- Passwords cannot be reused for 1 year

System-Level Passwords

- All system-level passwords must adhere to the following guidelines:
- Passwords must be changed at least every 6 months
- All administrator accounts must have 12 character passwords which must contain three of the four items: upper case, lower case, numbers, and special characters.
- Non-expiring passwords must be documented listing the requirements for those accounts. These accounts need to adhere to the same standards as administrator accounts.
- Administrators must not circumvent the Password Policy for the sake of ease of use

Password Protection /R

- The same password must not be used for multiple accounts.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential {COMPANY-NAME} information.
- Stored passwords must be encrypted.
- Passwords must not be inserted in e-mail messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords must not be revealed on questionnaires or security forms.
- Users must not hint at the format of a password (for example, “my family name”).
- {COMPANY-NAME} passwords must not be shared with anyone, including co-workers, managers, or family members, while on vacation.
- Passwords must not be written down and stored anywhere in any office. Passwords must not be stored in a file on a computer system or mobile device (phone, tablet) without encryption.
- If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
    - Take control of the passwords and protect them
    - Report the discovery to IT
- Users cannot circumvent password entry with an auto logon, application remembering, embedded scripts, or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup processes) with the approval of IT. For an exception to be approved, there must be a procedure to change the passwords.

- PCs must not be left unattended without enabling a password-protected screensaver or logging off the device.
- If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
    - Take control of the passwords and protect them
    - Report the discovery to IT /R
- Security tokens (i.e. smartcards, RSA hardware tokens, etc.) must be returned upon demand or upon termination of the relationship with {COMPANY-NAME}.

Application Development Standards

Application developers must ensure their programs follow security precautions in this policy and industry standards.