SMARTHEALTH

Password Policy

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 an agency's entire network. As such, all SMARTHEALTH employees (including contractors and vendors with access to SMARTHEALTH 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.

Scope

This guidance applies to all SMARTHEALTH employees, staff subordinate to SMARTHEALTH contracts, as well as any individual using SMARTHEALTH resources. This guidance applies to all network and computer systems (desktops, workstations, laptops, servers, firewalls, hubs, switches, and remote access devices) in the Local Area Network and stand-alone computers.

Password Policy

Creation of Passwords

- It must be at least 8 characters long, but not longer than 20 characters.
- It must not include Space, your NetID, First Name or Last Name.
- It must have at least one of each of the following:
    - Upper case letter
    - Lower case letter
    - Number
    - Special character among those listed below
      ! @ # $ ^ ( ) - + _ = | ` ~ [ ]

Changing Passwords

- It must be changed at least once a year.

Protecting a Password

- Passwords must be treated as confidential information.
- Passwords must not be included in email messages or other forms of electronic communication.

Sharing a Password

- Passwords are issued to individuals for their exclusive use, and they may not be shared.
- Passwords must be shared only with appropriately designated technical personnel.
- Users need to beware of "phishing" or other social engineering scams where a user may have his or her password requested over the phone. SMARTHEALTH technology personnel (i.e., IT Customer Service Center, ITSO, Technical Staff), as a best practice, do not request a user's password over the phone.

Reporting a Password Compromise

- Suspected compromises of passwords must be reported immediately to the SMARTHEALTH IT Customer Service Center at 4-5555.
- The password in question must be changed immediately.

Consequences

SMARTHEALTH employees who violate this policy may be subject to disciplinary action for misconduct and/or performance based on the administrative process appropriate to their employment

Contact

Chief Information Officer
smarthealthit@sm.com