PASSWORD SECURITY STANDARD

Security Standards: are mandatory security rules applicable to the defined scope with respect to the subject.

Overview

Passwords are an important aspect of computer security. They are the front-line of protection. A poorly chosen password or password behavior may result in the compromise of the University's network or exposure of sensitive information.

Scope

All authorized users who have or are responsible for an account on any University computer system including but not limited to faculty, staff, students, contractors or guests.

Purpose

The purpose of this document is to establish a standard for creating strong passwords, managing those passwords, and protecting the passwords.

Complexity

Within the limits of the operating system or application, passwords must:

- Contain a minimum of eight (8) characters.
- Contain characters from all four (4) of the following character types:
  - Upper case characters (A-Z).
  - Lower case characters (a-z).
  - Numerical characters (0-9).
  - Special characters (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./).

In addition, do not use passwords that contain:

- The login name or user’s name in any configuration
- Words found in a dictionary (English or foreign)
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Identifiable personal information, names of family, birthdays, addresses, phone numbers, etc.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Words preceded or followed by a digit (e.g., secret1, 1secret)
- Words spelled backwards.
- Slang, dialect, or jargon words from any language.
Management

The following password management practices must be followed and where technically possible, system controls must be configured as follows:

- Prevent password reuse with a history of the last 6 passwords.
- Maximum password age of 270 days.
- Minimum password age 3 days.
- Password complexity checking.
- Account lockout after 10 sequential invalid logon attempts.
- Account lockout duration for a minimum of 15 minutes.
- Must not store passwords in clear text or in any easily reversible form.
- Utilize TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever feasible.

Protection

Users are responsible for the following:

- Passwords should be memorized and never be written down or stored on-line (including smartphones, tablets, or similar devices) in an unsecured manner.
- Do not use the same passwords for University accounts as for other non-Health Science Center access (e.g., personal e-mail, social media, option trading, benefits, etc.), nor should you use the same password across all personal accounts.
  - The use of secure password managers is highly recommended. Products can be researched on the Internet, and Information Security can be contacted for recommendations.
- Do not reveal your personal password to ANYONE, including administrative assistants or management.
- Group passwords are prohibited unless an exemption is granted by the Chief Information Security Officer
  - Group passwords must be tightly managed and must facilitate individual accountability; however, ultimate responsibility resides with the owner.
- Never reveal a password electronically, such as an email message.
- Do not talk about a password in front of others.
- Do not use the "Remember Password" feature of applications (e-mail, browsers, etc.).
- Do not write passwords down and store them anywhere in your office.
- Be aware of attempts to steal passwords through social engineering or malware.
  - Social engineering through e-mail, or phishing, must be reported to Information Security by sending a copy to spam@uthscsa.edu.
If an account or password is suspected to have been compromised, report the incident to Information Security and change all passwords.

Avoid others watching you type your password (shoulder surfing).

---

**Examples**

One way to create a password is to use a song title, a movie title, song lyrics, an affirmation, a favorite quote, or other phrase, for example:

- "This May Be One Way To Remember" and the password could be: "Tmb1w2R!" or "Tmb1W>r~" or some other variation.
- "I want to retire a rich person someday" and the password could be: "Iw2Ra$ps".
- “Now is the time for all good men to come to the aid of their party” would be the quote, and the password could be “NitTf@gm2c2taotp!” or some variation.

Passwords should be long and complex enough to prevent guessing, but not so long and complicated they could be forgotten. Develop a password scheme that meets your needs.

---

**Exceptions**

Exceptions are granted on a case-by-case basis by the Chief Information Security Officer. Request an exemption by contacting Information Security by e-mail at InfoSec@uthscsa.edu.