UTSA Institutional Compliance
Office of Information Security

OIS 25 – Standard for Passphrase and Passwords

I. STANDARD STATEMENT

A. Passwords are a critical component of computer security, providing front-line protection for electronic resources by reducing unauthorized access. Passwords are required for all University computing devices that are connected to the network. It is always recommended to use passphrases when possible. Passphrases are required, in conjunction with the myUTSA ID, when accessing UTSA information resources.

B. A department and/or system administrator may implement a more restrictive policy on local systems where it is deemed appropriate or necessary for the security of confidential data.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

The Office of Information Security
informationsecurity@utsa.edu

V. PROCEDURES

A. PROTECTING PASSWORDS AND PASSPHRASES
1. Never share passphrases/passwords with anyone including family members, supervisors, co-workers, or OIT personnel.
2. Do not included passphrases/passwords in email messages unless authorized by the Office of Information Security (OIS).
3. Do not write passphrases/passwords down.
4. If passphrases/passwords must be stored, they must be encrypted.
5. Passphrases/passwords shall be treated as confidential information (Category 1).
6. Do not enter password/passphrase in forms or sites that look suspicious, always check legitimacy if not sure.

B. PASSPHRASES (Applies to passphrases used to login to myUTSA accounts)

1. Minimum Passphrase Requirements:
   a. Be at least 15 characters long.
   b. Be no more than 127 characters long.(Some applications limit the number of characters that can be used).
   c. Not be used for the user's other UTSA and non-UTSA accounts.
   d. Not consist of a common phrase.
   e. Not be based on something that's guessable by knowing you or by reviewing information about you.
   f. Not consist of letter or number patterns.
   g. Not be similar to the user's previous passphrases.
2. Highly Encouraged Passphrase Recommendations
   a. Use at least one: lower-case and upper-case letter, number and special character.
   b. Change passphrase on a periodic basis (i.e., quarterly, annually, etc.).
3. Passphrase Construction Options
   a. Create a passphrase consisting of several words that you can remember, but not easily guessable.
   b. Create a passphrase using the first letter of each word in a sentence that you can remember, but not easily guessable.

C. PASSWORDS (UTSA requires that any system employing user authentication via passwords must meet minimum requirements as stated below)

1. Minimum Password Requirements
   a. Contain at least 15 characters.
   b. Contain at least one upper- and lower-case character.
   c. Contain at least one number and special character (where applicable).
   d. Not be used for the other UTSA and non-UTSA accounts.
   e. Not be a word or acronym found in any dictionary.
   f. Not be based on personal information, names of family, birthdates, etc.
   g. Be changed every 180 days (Server/Application passwords only).
   h. Vendor/Application default passwords much be changed.

D. ACTIVE DIRECTORY CONFIGURATION (Applies to general network configuration regarding passphrases and passwords, where applicable).

1. Minimum Network Configurations
   a. Enforce Password History = 6 passwords
   b. Maximum Password Age = 0
   c. Minimum Password Age = 24 hours
   d. Minimum Password Length = 15
   e. Password Must Meet Complexity Requirement = none
   f. Store Passwords Using Reversible Encryption = Disabled

E. ADDITIONAL CONTROLS TO ENHANCE PASSPHRASES AND PASSWORDS

1. Multi-Factor Authentication (MFA) is to be applied, where practical or required, in combination with passphrases and passwords to further enhance protection of resources against unauthorized access.
2. If a passphrase, password or account is suspected of being compromised, OIS will initiate notification and any other steps deemed necessary to change the passphrase or password.

Title: OIS 25 – Standard for Passphrases and Passwords
Effective Date: October 7, 2010
Last Revised: August 5, 2020