THE UNIVERSITY OF TENNESSEE
MARTIN

UT - Martin Policy: IT1002-M - Password Standard	
Version: 8	Effective Date: 08/01/2023

Objective:

This standard establishes requirements and recommendations for the creation and protection of secure passwords.

Scope:

This standard applies to all users of, and information technology (IT) resources owned, operated, or provided by the University of Tennessee at Martin (UTM) including its regional centers.

"Users" includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University's information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles:

The University has chosen to adopt the policy principles established in the National Institute of Standards and Technology (NIST) 800 series of publications, and this standard is based on those guidelines. Specifically, this standard is based on guidelines in *NIST SP 800-53 Revision 5.1, Recommended Security Controls for Information Systems and Organizations.*

UTM must develop or adopt and adhere to a program that demonstrates compliance with related policies and standards. This standard is the responsibility of the Position of Authority.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of this policy is assumed if a User accesses, uses, or handles University resources.

UT - Martin Policy: IT1002-M - Password Standard	
Version: 8	Effective Date: 08/01/2023

Protection:

Passwords must never be written down or recorded. Users must never share or divulge their password to anyone. Each user is accountable and responsible for any action taken with their account. No University employee or administrator should ever ask a user for their password, and if such an action takes place, the user should not reveal it to anyone, no matter how plausible the reason. Any password that is known or suspected to be compromised must be changed immediately.

Length:

Password length is one of the main factors that determines password strength. All passwords must be a minimum of twelve (12) characters (IA-5.1).

Complexity:

Easy to guess words, such as single dictionary words, university name, product or service names, the user's proper name or username, must not be used at any time. Strong passwords should include at least three of the following characteristics (IA-5.1):

- At least one numeric character,
- At least one special character (!, @, #, $, <space>, etc.),
- At least one lower case character,
- At least one upper case character.

Single dictionary words and short words with substituted characters do not make good passwords even though they meet the complexity requirements. Examples of bad passwords include:

- Abbreviation!
- R3fr1g3rat0r*
- Interm3d14t3

Examples of strong passwords (longer passwords are more secure):

Random, unrelated words with numbers and special characters can be hard to recall:

- Parity.Mint3126@
- Lighter>volume~Argument83#
- CalibrationProducesClimbing620^

Randomly generated character strings are hardest to recall:

- A83dXD8*X5$3tSd
- 3A^6yS6sT3P8QAta*r
- WrRdwR68x4y^5eG@#^GU3

A passphrase is the strongest yet easier to recall:

- How much wood would a woodchuck chuck if it played baseball?
- The balanced crusader angelfish recoiled.
- A cable shrimp retail saucer!

DO NOT use any of the previous examples as your password.

Expiration (IA-5):

All passwords generated within UTM must be set to expire at a maximum of every 180 days. Passwords used for privileged accounts on information systems must be set to expire at a maximum of 90 days. Passwords generated within UTM for access to Confidential information must be set to expire at a maximum of every 60 days.

However, when a user enables Two-Factor Authentication (2FA) for their account, the password will not expire after the next time it is changed.

Passwords issued for temporary accounts, password resets, and locked out IDs must all be reset and require users to change their passwords at the next login.

Uniqueness:

Where technically feasible, a history of at least ten (10) passwords must be kept within the system for each password generated.

Work and Personal Separation:

Users must never use the same passwords between university/work and personal accounts. This creates the risk of unauthorized parties gaining access to university systems.

Recommendation:

It is highly recommended that users implement unique passwords for each account. It is common practice for threat actors to try compromised credentials in multiple services to gain access to additional accounts. Never reuse credentials that have been compromised.

Account Lockout (AC-7):

Active Directory / General Logins

An account will be locked out after thirty (30) failed login attempts in fifteen (15) minutes. The account will remain locked for fifteen (15) minutes once locked.

Banner / Oracle Logins

Accounts will be locked out after five (5) failed login attempts. The account will remain locked for fifteen (15) days or until it is unlocked by an administrator.

Compromised Default Passwords:

If a users' default credentials are compromised, the flag must be set on their account to block it from being reset to the default.

Display and Printing:

The display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them (IA-6).

Cracking:

Users must not attempt to "break", "hack", "crack", or otherwise determine another user's password. This applies to passwords for faculty, staff, students, friends, and accounts on external systems.

Encryption:

Passwords used to access sensitive information must not be sent across the network in clear text. Passwords must not be listed in clear text for the purpose of automating a login sequence. All passwords must be stored in an encrypted format by the OS, DBMS, or application.

NOTE: All encryption methods and technology must comply with regulations governing this technology.

Retrieval:

Computer and communication systems must be designed, tested, and controlled to prevent the retrieval of stored passwords.

Information System Installation:

Default authenticators must be changed upon information system installation, by requiring developers and/or installers to provide unique authenticators or change default authenticators for system components prior to delivery and/or installation (IA-5).

Service Accounts:

Passwords issued for service accounts not requiring a regular login must conform to a stricter standard. At minimum, they should contain at least 3 unrelated random words, 3 numbers, and one special character.

New Hire 2FA:

New employees have 30 days after hiring to enroll in 2FA, after which their account will be automatically enabled.

Exceptions:

Some systems may not be able to comply with this policy due to restrictions of password length or unsupported characters. For these systems, an exception must be noted and approved by the Security Team.

Approved Password Managers:

The use of a password manager is allowed and encouraged for securely generating and recalling strong, unique passwords and passphrases. The following password managers have been approved for use with required authentication requirements:

- Online – Keeper (UT), 1Password, Bitwarden, LastPass
  - Must have complex password with at least sixteen (16) characters
  - Must use Two-Factor Authentication (2FA)

- Offline - KeePass, KeePassX
  - Must have complex password with at least sixteen (16) characters
  - Must require a key file that is stored separately from the database file
  - Applications must be kept updated to the latest versions

Others not listed must be approved by the Security Team before implementation.

UT - Martin Policy: IT1002-M - Password Standard	
Version: 8	Effective Date: 08/01/2023

References:

IT0132 - Identification and Authentication

IT0132-M - Identification and Authentication Program

NIST SP 800-53 Revision 5.1, Recommended Security Controls for Information Systems and Organizations

NIST SP 800-63B Digital Identity Guidelines - Authentication and Lifecycle Management, Appendix A – Strength of Memorized Secrets

Definitions:

Cracking: Refers to using various methods to reveal a password with the intent of accessing a computer, system, or service to which one is not authorized.

Encryption: The process of converting information or data into a special form to prevent unauthorized access.

Passphrase: A string of words used to gain access to a computer system or service.

Password: A string of characters supplied by a user to gain access to a computer, computer system, or electronic device. Also referred to as a Memorized Secret.

Password Manager: An application used to organize, encrypt, and generate passwords.

Threat Actor: An entity, internal, external, or partner, that is partially or wholly responsible for an incident that impacts, or has the potential to impact, the safety or security of another entity, person, or organization.

Two-Factor Authentication (2FA): A method of confirming a user's claimed identity by requiring a combination of two different components, which includes something you know (password, PIN), something you have (smart card, token), and something you are (biometrics).