Policy Title: IT6011 - Password Policy

Subject Area: Information Technology

Responsible Official(s): Chief Information Officer

Responsible Office(s): Information Technology Services

Policy Statement

The purpose of this password policy is to establish a standard for the creation, protection, and use of passwords to secure the institution's information systems and data. The University of Memphis is committed to maintaining a secure and reliable computing environment to protect the integrity, confidentiality, and availability of its information systems and data. As part of this commitment, we require all users, including students, faculty, staff, contractors, and other affiliates, to adhere to the following password policy. This policy outlines the requirements for creating, maintaining, and securing passwords that are used to access the institution's systems and services.

The implementation of strong password practices is critical to safeguarding sensitive information and preventing unauthorized access. Compliance with this policy is mandatory for all members of the UofM community. Failure to comply may result in disciplinary action and/or restricted access to institutional resources.

This policy will be reviewed regularly to adapt to evolving security challenges and technological advancements. We encourage all users to exercise due diligence in securing their passwords and to promptly report to IT Security any security concerns.

Definitions

Password Manager

A **password manager** is a software tool designed to store, manage, and organize passwords and login credentials for various online accounts. It helps users create strong, unique passwords for each account and securely stores them in an encrypted database, accessible only with a master password. A password manager is designed to enhance digital security and simplify the process of managing numerous passwords, reducing the risk of password-related breaches. Key features of a password manager often include:

- **Password Generation**: Generates strong, random passwords to enhance security.
- **Secure Storage**: Uses encryption to protect stored passwords and sensitive information.
- **Autofill and Auto-login**: Automatically fills in login details on websites and applications.
- **Cross-platform Synchronization**: Syncs password data across multiple devices, allowing access from anywhere.
- **Security Alerts**: Notifies users of potential security breaches or weak passwords.

Policy

Password Requirements

Password Complexity

Passwords must meet the following complexity requirements:

- **Length**: between 15-64 characters long
- **Composition**: Must include at least three of the following:
    - Uppercase letters (A-Z)
    - Lowercase letters (a-z)
    - Numbers (0-9)
    - Special characters (_! $ % ^ * + -)
- **Prohibited Elements**
    - Must not include easily guessable information such as the user's username, first or last name, or familiar words and phrases.
- **Password Change Frequency**
    - **Expiration**: Passwords do not expire, but must be changed when there is suspicious activity associated with the account. IT Security will force a password reset in this instance.
    - **Notification**: Users will receive a notification if IT Security has initiated a password reset.
- **Password History and Reuse**
    - **History**: Users cannot reuse any of their previous passwords.
    - **Reuse**: Passwords should not be reused across different accounts or systems within the institution.
- **Account Lockout Process**
    - **Lockout Threshold**: Accounts will be locked after 5 consecutive failed login attempts.
    - **Lockout Duration**: Accounts will remain locked for 5 minutes or until an authorized administrator resets the account.

Password Management

Password Storage and Transmission

- **Storage**: Passwords must not be stored in plain text. They must be stored using industry-standard hashing and salting techniques. Hashing techniques for passwords involve using cryptographic hash functions which are designed to be slow and

computationally intensive. Salting adds an additional layer of security by appending a unique, random value to each password before hashing, ensuring that identical passwords produce different hash values and protecting against precomputed attacks.

- **Transmission**: Passwords must not be sent via email or any other unsecured methods. Passwords must be entered on secure, encrypted (HTTPS) pages.

Use of Password Manager

- Although the University does not offer or recommend a specific password manager, Users are encouraged to use password managers to securely store and manage passwords.

Multi-Factor Authentication (MFA)

- MFA must be enabled for accessing sensitive systems and data. MFA provides an additional layer of security beyond passwords. Systems that use the institution's SSO service are included in MFA protection by default.

Policy Violations

- Non-compliance with this policy may result in disciplinary actions, including but not limited to suspension of access to IT resources, academic penalties in accordance with the institution's policies and other disciplinary actions up to and including termination.

Roles and Responsibilities

User Responsibilities

- Users are responsible for maintaining the confidentiality of their passwords and must not share them with others.
- Users must report any suspicious activities or suspected security incidents involving their accounts immediately to the IT Security Team.

IT Security's Responsibilities

- IT Security is responsible for enforcing this policy, providing support for secure password management, and regularly reviewing and updating security measures.
- IT Security conducts regular security awareness training, including best practices for password creation and management, in accordance with IT6009 - Information Technology Security Awareness Training Program

Related Documents, Policies and Forms

IT6000 - Data Access
IT6003 - Acceptable Use of Information Technology Resources
IT6004 - Security and Protection of Electronic Information Resources
IT6005 – Data Security Policy
IT6009 - Information Technology Security Awareness Training Program
ITS Security Procedures and Best Practices

State of Tennessee Data Security Law

Last Revision Update Log: 11/12/2024