University Password Standards and Guidelines

**Purpose:** To provide a set of minimum security standards governing the use of passwords for University of Connecticut information technology systems. This document is intended to offer guidance for system and application administrators. All parties are encouraged to apply more stringent controls than those outlined below, though this is not a requirement.

**Software Compatibility and Limitations**

It is recognized that software applications offer many varied capabilities with respect to authentication, authorization, role-based access control, password complexity, account management, and auditing of these components. Many examples of software exist which will not be able to conform to some aspect of the following guidelines. Despite these deficiencies, such software is commonly necessary for performing critical functions. Reasonable efforts should be made to improve the security posture of such software by enhancing system configurations over time, engaging with vendors, and developing auditing capabilities when possible and feasible. It is encouraged that administrators contact the Information Security Office for evaluation of systems, applications, or accounts lacking the technical capability to meet the requirements below; the ISO will offer guidance for selecting the best and most secure configuration within the limitations of the given system.

**NetID Password Standards**

*Scope and Intent*

This section is intended to provide guidance for systems and applications which utilize university NetID infrastructure for authentication and authorization purposes.

*Password requirements*

- Passwords must never be stored in plain text.
- Passwords should not be displayed in plain text as they are being entered.
- Passwords must be encrypted and/or hashed while in transit to the authenticating system.
- Passwords shall contain at least 8 characters.
- Passwords shall be composed of representatives of the following character sets: upper case, lower case, numeric characters, and/or punctuation.
- Password controls shall lockout user accounts after 10 consecutive unsuccessful login attempts for a period of at least 60 seconds.

**System Administrator Password Standards**

*Scope and Intent*

This section is intended to provide guidance for systems and applications which utilize local/internal authentication and authorization. It is recommended that these requirements be used to evaluate software being considered for acquisition and plan for software under development.

*General requirements*

- Information Technology administrators must utilize a dedicated system administration account for administrative duties, separate from their general purpose account.
Credential requirements

- Passwords must never be stored in plain text.
- Passwords must not be displayed in plain text as they are being entered.
- Passwords must be encrypted and/or hashed while in transit to the authenticating system.
- Passwords shall contain at least 10 characters.
- Passwords shall be composed of representatives of the following character sets: upper case, lower case, numeric characters, and/or punctuation.
- Password controls shall lockout user accounts after 10 consecutive unsuccessful login attempts for a period of at least 60 seconds.

Service Account Password Standards

Scope and Intent
This section is intended to provide guidance for systems and applications which require service and/or machine accounts for automation, monitoring, and other non-interactive tasks not performed by an individual.

Credential requirements

- Credentials should never be stored in an unprotected manner.
  - If plain-text credentials are required for purposes of automation, controls must be in place to prevent unprivileged access to the credentials (e.g., file system access controls)
  - In place of a password, an alternative such as a cryptographic key may be used for authentication and authorization.
- Credentials must not be displayed in plain text as they are being entered.
- Credentials must be encrypted and/or hashed while in transit to the authenticating system.
- Service accounts should never be used as a user account through an interactive logon mechanism except for testing purposes.
- Passwords shall at least contain 16 characters.
- Passwords shall be composed of representatives of the following character sets: upper case, lower case, numeric characters, and/or punctuation.
- Service accounts must have a responsible point of contact at an individual or group.
- Service accounts should be reviewed bi-annually to ensure remain necessary and meet the above requirements. Those deemed unnecessary should be deactivated and/or removed.
- Service accounts which are themselves provisioned using the same mechanisms used for administrator accounts must nevertheless conform to the requirements above.
Initial Account Provisioning

Newly provisioned user accounts must have a secure password set by the account holder. This may be accomplished via an activation method that allows the account holder to set a password (before which the account is not usable), secure transmission of an initial password to the account holder, a small expiration window for an initial password, and/or manual intervention of support resources.

If an initial account password is set before account handoff to the account holder:

• Account holders must have the ability to either activate an account and set a password before use or require users to set a password during initial access to a system. Service accounts may be considered exempt from this requirement.

• All vendor-supplied passwords, including service accounts, must be changed as soon as possible after system/application deployment and before becoming operational.

Password Distribution

To ensure that the intended account holder is the recipient of a password or credential, distribution should occur only after reasonable effort has been made to verify the identity of the account holder.

Individuals should be confirmed as the intended recipient by contact via an authorized work phone number, verification of personal data, photo ID, or any similar means.

Passwords may be communicated via:

• mail (sealed envelope) is authorized to distribute passwords

• encrypted file transfer (e.g., Filelocker or similar) may be used to securely distribute passwords.

• Verbal conversation, phone call to authorized work telephone number, etc.

Password Protection

• When visiting web sites not affiliated with the University, individuals should create a password different from his/her NetID password.

• Individuals should not share passwords with others; multiple users should not share the same user account.

• It is understood that hardcopy records of such information may be necessary for disaster recovery or similar. Securely store paperwork that includes user ID and password information. When no longer needed, securely dispose of such documentation.

• Do not save passwords within an application (e.g., a tablet/cell phone or browser) unless the device is protected against misuse by other parties by a separate login or pin.

• Use of secure password managers are encouraged.