1. PURPOSE OF PROCEDURE

This document describes the minimum authentication standards that must be met by University of Wisconsin (UW) System institutions.

2. RESPONSIBLE UW SYSTEM OFFICER

Associate Vice President for Information Security

3. DEFINITIONS

The following key terms are presented in this standard. Please refer to the UW System Information Security Program Glossary for the following definitions:

- Multi-factor Authentication (MFA)

**Account Types:** While each institution will have varying account types by title, all accounts fall into one or more of the 4 categories below. The type and usage of an account generally determines its authentication requirements. In order to distinguish between requirements based on account type, this Standard refers to several different kinds of accounts according to the following definitions.

- **User Accounts:** are those under the control of a specific individual and are not accessible to others. These are user-interactive accounts.
- **Shared Accounts:** An account that can be accessed by multiple individuals to allow them to appear as a single business entity or accomplish a single shared function. These are user-interactive accounts.
- **Privileged Accounts:** A qualifier used to describe User Accounts and Shared Accounts that have elevated access to configure or significantly change the behavior of a computing system, device, application or other aspect of the Information Technology
(IT) resource or IT infrastructure. These accounts should be considered highly sensitive. These are user-interactive accounts.

- **Service Accounts:** Accounts that are intended for automated processes such as running batch jobs or applications or establishing connections between web, application, and database servers, or external applications or services. To be considered a service account, the account must not be primarily used for general login to systems by users.

**Passphrase:** A secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity. A passphrase is similar to a password in usage but is generally longer for added security.

**Password:** A secret that a claimant uses to authenticate his or her identity. Passwords are typically character strings.

**Secret:** Commonly referred to as a passphrase, password, or if numeric, a PIN. A secret value of sufficient complexity and secrecy intended to be impractical for an attacker to guess or otherwise discover the correct secret value.

4. **PROCEDURES**

**A. STANDARDS**

1. **Minimum Password and Passphrase Requirements**

For authentication systems that use passwords or passphrases as an authenticator type, the following password and passphrase length requirements represent a minimum standard for UW System accounts. System password and passphrase requirements must also meet or exceed all applicable federal statutes and administrative code, and other applicable industry standards, such as Payment Card Industry Data Security Standards, that apply to those systems.

<table>
<thead>
<tr>
<th>Account Type*</th>
<th>Minimum Length Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Accounts (Minimum Baseline)</td>
<td>12</td>
</tr>
<tr>
<td>Privileged Accounts and accounts with access to high risk data</td>
<td>14</td>
</tr>
<tr>
<td>Service Accounts</td>
<td>16</td>
</tr>
</tbody>
</table>

*Note that whether an account is classified as a user account or a shared account does not affect password and passphrase length requirements.*

Additionally, passwords and passphrases must:
• Not contain the accounts username or other account identifier;
• Be compared against a dictionary of weak or known passwords, if such functionality natively exists in the authentication system; and
• Enforce history requirements, such that secrets associated with accounts must not be the same as any of the last 24 secrets for that account.

II. Session Reauthentication

Periodic reauthentication of sessions must be performed at various time intervals in addition to elapsed periods of user inactivity. Users accessing moderate or high risk data must reauthenticate to the application hosting the data at least once per 12 hours during an extended usage session, regardless of user activity. Reauthentication procedures must be commensurate with the initial authentication process used to access the application.

Users must also reauthenticate following any period of inactivity lasting 30 minutes or longer while accessing moderate or high-risk data.

The session must be terminated (i.e., logged out) when either of these time limits are reached.

III. Account Lockout Requirements

Public facing authentication systems, those of which allow for authentication from outside of institution networks, must include an account lockout mechanism to be triggered after a maximum of 14 invalid secret entries. Administrators may choose to have a time-based lockout (minimum 5 minutes) or a hard lockout which requires the user to follow a process to reset their secret. Alternatively, risk-based or adaptive authentication techniques may be used to identify user behavior that falls within, or out of, typical norms, and enforce lockouts accordingly.

IV. Multifactor Authentication

User accounts and shared accounts that are used to access high risk data must use MFA. This requirement does not apply when students are exclusively accessing their own information.

Privileged accounts, excluding service accounts, must also use MFA.

V. Frequency of Secret Changes

When MFA is not incorporated into all internet-facing instances when an account is used, secrets must be changed on a regular basis, in accordance with the following:
### Account Type

<table>
<thead>
<tr>
<th>Account Type</th>
<th>Secret Change Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Account</td>
<td>5 Years</td>
</tr>
<tr>
<td>All Other Accounts</td>
<td>Annually</td>
</tr>
</tbody>
</table>

Secrets **must** be changed immediately if a compromise of credentials has been independently discovered, publicly disclosed, suspected, or if a device has been lost or stolen. This includes discovery of plaintext and/or hashed secrets.

Initial secrets that are provisioned for new user accounts must be changed during first use or, if not technically feasible, within five business days of first use.

Default, non-unique secrets for accounts that are embedded in new devices or applications must be changed during initial device or application configuration, or if not technically feasible, within five business days of device or application activation, unless those accounts are locked.

Service account secrets and shared account secrets must be changed within five business days when an employee with knowledge of said secrets:

- changes roles where knowledge of the secret is no longer necessary; or
- discontinues employment with UW System and/or its institutions. This requirement does not apply for systems that are inaccessible from outside the institution network.

### VI. Shared Accounts

Shared accounts should not be used to access high risk data and should be avoided when accessing moderate risk data. If, due to system limitations or problems, a shared account must be used, the institution must establish procedures for documenting, approving, and monitoring the use of shared accounts.

### VII. Requirements for Continued Account Access

Accounts must only remain active while there is a valid business justification for having the account. However, there may be times where accounts need to remain active past their normal defined periods:

- Individuals who leave employment in good standing **and** retain a documented affiliation with the university (emeriti, sponsorship, retiree/annuitant, adjunct faculty, instructional staff/faculty, etc.) may retain account access provided the following conditions are met:
An individual's affiliation must be formally documented and verified at least once every 365 calendar days
- Individuals retain access to campus IT resources/services, limited to those commensurate with their role
- Individuals remain subject to Board of Regents policies
- Individuals are required to annually complete information security awareness training
- Access will be disabled after 1 year of inactivity based on last login date

- Access for individuals who leave employment in good standing and do not retain a documented affiliation with the University, will be disabled on the termination date set in the Human Resource System. Access for these individuals may be retained for a period of up to 90 days to facilitate grade appeal process, if applicable.
- Access for individuals who are discharged with no notice and/or terminated for cause must be revoked immediately. If a criminal offense is involved in the termination, the UW System Office of General Counsel or an institution's legal affairs office must be consulted to ensure no legal hold on account information, files, etc. is required.

VII. Storage of Secrets

Chief Information Officers (CIO) or their designee may approve the use of password managers or software applications designed to manage user secrets securely. Password managers must meet the following minimum security requirements:

- Password managers shared between team members must utilize logging to uniquely identify employee access to the manager and access of secrets within the manager
- Password manager authentication procedures must be commensurate with the authentication requirements for the accounts the password manager stores. For example, if the password manager will store privileged account credentials or credentials for accounts that have access to high risk data, the password manager must require MFA and meet the associated secret requirements specified in this policy.

Secrets must be encrypted when stored electronically. Secrets must not be written down unless secured in a manner that restricts unauthorized individuals from accessing the secrets.

5. RELATED DOCUMENTS

UW System Administrative Policy 1030, Information Security: Authentication
6. HISTORY

Revision 4: October 4, 2019
Revision 3: January 09, 2019
Revision 2: January 25, 2018
Revision 1: July 31, 2017
First Approved: September 14, 2016

APPROVED BY:

__________________________
Robert G. Cramer
Vice President for Administration
University of Wisconsin System