Information Resources Division
UIW STANDARD FOR IDENTIFICATION, AUTHENTICATION AND PASSWORDS

Effective Date: March 8, 2018
Contact: Brian Anderson, Director of Information Security

INTRODUCTION

User authentication is a means to control who has access to information resources. The confidentiality, integrity, and availability of information can be lost when access is gained by a non-authorized entity. This, in turn, may result in loss of revenue, liability, loss of trust, or embarrassment to the university. Authentication factors include something you know, something you have, and something you are. This standard defines the minimum requirements for authentication.

SCOPE

This standard applies to university information technology resources. It further applies to all users of those systems. This includes: faculty, staff, administrators, students, volunteers, contracted employees and other university affiliates privileged to use university information resources. In addition to this policy, all users of information and computing resources at UIW are also responsible for adherence to any State or Federal regulations regarding computer use at the university.

STANDARDS

Minimum Password Standards

All systems shall have passwords that conform to the following password rules:

- Not contain any part of the user's account name, PIDM, SSN, or date of birth
- Be at least eight characters in length
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example: !, $, #, %)

Privileged Account Password Standard

Accounts with privileged or administrative access to a resource will conform to the standard above, but have a minimum length of 12 characters

Service Account Password Standard

Service account passwords may be set to never expire but must have a minimum password length of 20 characters and must be randomly generated using the complexity standards above.

Service account passwords must be changed when any employee with access to those passwords is terminated from employment with the university.

Windows Local Administrator Passwords
Local administrator passwords on university systems will be different on each system. These passwords must comply with the minimum password standards and be changed every 120 days.

Password History
Password history must be maintained in a manner that prohibits the 10 previous passwords from being reused.

Password Expiration
Passwords must expire after 120 days

Password Confidentiality
Stored passwords must be encrypted or hashed with an appropriately effective algorithm.

Passwords must be treated as confidential information. Passwords may not be shared with or revealed to anyone.

Passwords should never be transmitted as plain text.

If the security of a password is in doubt, the password must be changed immediately.

If a password has been compromised, the incident should be reported to the Information Security Office immediately.

Passwords may not be embedded in scripts, or hard-coded in client software for systems that process/store critical and/or confidential data. Exceptions may be made for specific applications (like automated backup) with the approval of the information resource owner.

New Password Issuance
Passwords created by the help desk or other password-issuing entity must be completely random and not based on any information about the user. These passwords must conform to the minimum password standards described above.

Automated password-issuing systems must generate random passwords. These passwords must conform to the minimum password standards described above.

Users of university systems must be forced to change their password upon first login to the system after a new password has been issued.

Failed Logon Response
University resources must be configured, where possible, to lock out users after 10 unsuccessful login attempts

Upon being locked out, the user must not be automatically unlocked for a minimum of 15 minutes.

Screen and Service Locking
Computing devices must have timed screen-lock or auto logout configured to engage after a period of 30 minutes of inactivity. The exception to this is presentation and classroom systems where a screen lock would cause disruption. In this case, the timer may be extended to minimize disruption.

Self-Service Password Reset
Self-Service password management tools must use a minimum of one of the following factors to authenticate users attempting to reset passwords. These factors may include, in preferential order:

- Multifactor authentication mechanism (physical token, Duo, Azure MFA, etc.)
- Token sent via text message to a pre-configured mobile number
- Token sent via email to a pre-configured secondary email address
- Pre-configured security questions

Systems relying on security questions to reset passwords must have a brute-force prevention mechanism in place.

Self-service password management and automated password generation tools should have, where the capability exists, auditable transaction logs containing information such as:

- Time and date of password change, expiration, administrative reset;
- Type of action performed; and,
- Source system (e.g., IP and/or MAC address) that originated the change request.

Manual Password Reset
Users requesting a password reset must be positively identified via one of the following mechanisms, in preferential order:

- Visual verification of University or government issued identification card
- Verification of preconfigured security questions
- Verification of personal information (last 4, address, phone number)

First Approved: March 8, 2018, version 1.0
Revised: