Password Policy (ISP-06)

Document Owner

Executive Owner:	Darrell Morrison
Functional Area:	Information Technology

Authorization

Authorized By:	David J. Hinson
Position:	Interim Chief Information Officer
Signature	
Authorization Date	02/25/2025

Version History

Issue	Reason For Change	Date
1.0	Initial Release	02/25/2025

Review Period

Information Security Policies are to be reviewed at a minimum annually.

Change Control

Requests for changes to Information Security Policies are to be sent to the document owner providing details of the requested changes and a short justification.

Exceptions

Requests for exceptions to this policy are to be submitted in accordance with the exception policy. Note that all exceptions are time limited to no more than 12 months in duration.

Applicability

This policy applies to all faculty, staff, students, and contractors who are issued access to University Information Systems, resources and services.

Table of Contents

Introduction

Authentication of user access to information systems is achieved by using a combination of something you are, something you have and something you know i.e. a password. Passwords themselves are easily circumvented if some basic standards and processes are not followed and as a result password policy is required to ensure passwords are secure enough to reduce risk of compromise and information exposure.

Objective

The objective of this policy is to define the password length, complexity and lifecycle requirements for accessing University IT services.

Policy Statement

General

Password length and complexity determine how easily an adversary can guess or break a password. That said arbitrarily long and complex passwords are difficult for users to remember.

- Adoption of the Azure active directory single sign-on (SSO) solution is mandatory for all applications as this reduces the need for users to remember and maintain multiple passwords.
- Where the SSO solution cannot be implemented, an exception is to be raised, and unique passwords are to be used for each application not part of the SSO solution.
- Users will be responsible for safeguarding their passwords and shall change passwords whenever there is any suspicion they have been compromised.
- Passwords are not to be shared with any other individual, not even members of the IT security team.
- System users may make use of password vaults only if administration of those vaults is controlled by a multifactor authentication mechanism.
- Users are never to write down (Other than in a vault, see above) or leave their passwords unprotected or visible to others. Examples are local files, contacts, or encrypted one drive folders and similar.

User Account Passwords

User passwords are those associated with enterprise applications such as M365 and finance systems. User passwords are to be a minimum of 8 characters or more, and contain at least one capital letter, one number and one lower case character. Users are encouraged to use random letter combinations or a phrase consisting of at least 4 words and not simple co-joined words.

- Password reset requests are either handled via the self-service password reset tool, or via a service request handled by the Helpdesk.
- Accounts will be locked out after not more than seven invalid logon attempts.
- Once a user account is locked out, it remains locked for fifteen (15) minutes or until the system administrator resets the account.
- User passwords are to be reset at least every 90 days.
- Passwords are not to be reuseable for at least 6 rotations.
- End-user support team members may share the initial log in password with new users over a telephone call. That initial password shall be set to require resetting on first log on and shall only be valid for 24 hours.

Admin Account – Human Accounts and Passwords

Admin accounts are those privileged accounts used by human engineers and operators to interact with, configure and maintain University Information Systems. The goal is for all such accounts to be accessed via a single sign-on solution. These accounts have extended powers and need to be judiciously guarded and carefully secured.

1. Administrator passwords are to contain 12 characters, or more and contain at least one capital letter, one special character and one lower case character.
2. Multifactor Authentication is to be enabled for all Administrator work in addition to the user ID and password
3. Accounts will be locked out after not more than 3 invalid logon attempts.
4. Require that once a user account is locked out, it remains locked for Sixty (60) minutes or until the system administrator resets the account.
5. Admin passwords are to be reset at least every 60 days.
6. Passwords are not to be re-useable for at least 10 rotations.

Admin Account – Non-Human Service Accounts and Passwords

Service or system accounts and passwords are for non-human or machine access and are required for a number of the services that the University utilizes that are not fully integrated with the AD-SSO solution. This includes database accounts and credentials as well as external vendor API keys, as well as hard coded administrative accounts commonly referred to as the root account. Root accounts are only to be accessed under break-glass situations. Service accounts are usually privileged accounts with widespread permissions and as such they need to be safeguarded carefully.

1. All service account details and passwords are to be stored in a Secrets Manager Vault.
2. Secrets are not to be hard coded into applications but are to be called at run time from the Secrets Vault.
3. Passwords are to be machine generated and totally randomized.
4. Passwords are to be at least 18 characters.
5. Service Account passwords are to include at least 3 of each of the following Special Characters, Numbers, Lower case characters, and Upper-case characters.
6. Service account passwords are to be rotated, i.e. changed every 180 days.

Laptop Mobile and Tablet Screen Lock Requirements

All devices used to access University Information Systems and data shall have a security screen lock that auto enables after 30 minutes of inactivity. The following are acceptable forms of device lock:

7. PIN code with minimum of 6 numerals
8. Password that meets criteria above
9. Fingerprint scanning
10. Facial Recognition
11. Screen lock PINs and passwords are to be changed every 180 days and are not to be re-used for 8 rotations.