FLORIDA
INTERNATIONAL
UNIVERSITY

Password & Account Management Standard

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
May 15, 2023	*May 5, 2023*	Division of Information Technology/IT Security Office

POLICY STATEMENT

This Password and Account Management Policy aims to provide a comprehensive framework for the proper creation, maintenance, and protection of user accounts and passwords within our organization.

POLICY SCOPE

This Policy applies to all user accounts on FIU systems, devices, and/or applications at FIU used by but not limited to students, faculty, staff, third party affiliates (consultants, vendors, Person of Interest), vendors, contractors, sub-contractors, suppliers, business partners, and other persons affiliated with FIU.

REASON FOR POLICY

The reason for this policy is to establish standards for the creation, usage, and management of user accounts and passwords, to reduce the risk of unauthorized access, data breaches, and other security incidents.

DEFINITIONS

TERM	DEFINITIONS
MFA (Multi Factor Authentication)	Multi Factor Authentication or Two-Factor Authentication (2FA) increases security on your FIU account by requiring you to log on by using both your password and your device (e.g. mobile phone or hardware token). Because it requires two steps to log in, 2FA offers more account security than a password alone - it provides added protection for both individuals and the FIU community at large.
Member or Member of the FIU Community	An authorized user of an FIU enterprise resource; includes faculty, staff, POI, contractors, students, volunteers.
FIU Systems	Any system and/or application on prem or in the cloud which FIU users authenticate to.

FIU Users	Students, faculty, staff, third party affiliates (consultants, vendors, Person of Interest), vendors, contractors, sub-contractors, suppliers, business partners, and other persons affiliated with FIU

ROLES AND RESPONSIBILITIES

Password Policy:

- Systems should observe these password age standards via technical controls:
  - Protected with MFA – No expiration
  - Without MFA protection – Expire at least every 365 days
- Minimum password length: 16 characters.
- Password composition must include lowercase letters, uppercase letters, numbers and special characters. Allowable special characters are **~!@#$%^&*()_+|`-=\{}[]:”;’<>?,./** and the **space character** (depending on system support).
- Enforce password history: 10 passwords remembered, where possible.
- Members must not share FIU accounts, passwords, secrets, credential, certificate, personal identification numbers, security tokens, smart cards, identification badges or other devices used for identification and authentication purposes.
- Passwords shall not be written down or stored without encryption.
- Passwords shall be changed immediately in the event of known or suspected (compromise or breach) or if disclosed to another party.
- Default or preconfigured passwords should never be used (e.g., manufacturer default passwords, default SNMP strings, etc).
- Manual password resets should be performed using randomized passwords every time.
- All passwords must be treated as Confidential information and should not be shared with anyone.

Account Lockout Protection:

- Where possible all the following should be configured:
  - Attempts to guess a password should be limited to ten (10) failed logins. Any attempts over ten (10) failed logins within 5 minutes (lockout counter reset time period) should automatically disable and/or lock the account. Account should remain locked (lockout time) for 15 minutes before a password can be attempted again.

Internet Facing Applications:

- In addition to password, lockout, and account management policies, University applications which are available from the Internet must be protected using a DoIT Information Security approved multifactor authentication provider.

Account and Access Management:

- A process shall be established to ensure a lifecycle of user accounts, and the removal of access after resignation / termination.
- A process should be in place to disable user accounts upon HR inactive status or after 90 days of inactivity (OneCard Building Access & FIU Network Account).
- Access provisioned through automation based on attributes (IE Job Title or function) must have formal documented approval by a data owner with the attributes defined.
- A process should be in place to ensure that systems terminate user sessions or require the user to reenter their password after 15 minutes of inactivity has been reached.
- Additional safeguards must be implemented to protect accounts of elevated or privileged access.
- FIU users requesting a Person of Interest (POI) account must ensure that the account is only active during the time period needed.

RELATED RESOURCES

- *https://pages.nist.gov/800-63-3/sp800-63b.html “Memorized Secret Verifiers” (Passwords)*

CONTACTS

Division of Information Technology
IT Security Office
11200 SW 8 ST, PC534
Miami, FL 33199
Security@fiu.edu
305-348-1366
https://security.fiu.edu

HISTORY

5/15/2023 - Initial Effective Date