



Authorization, Authentication and Access Management Policy

(Replaces Password Policy)

Responsible Office: University Systems and Networking Effective Date: 11/1/2023

Responsible Officials: Associate Vice President Last Revision: New Policy
Director of Systems Last Review:

Section A – University Systems and Applications

I. Purpose

The purpose of this policy is to establish information security standards for individuals receiving credentials to Fairleigh Dickinson University ("FDU" or "University") resources and how those resources are accessed.

II. Scope and Applicability

This policy applies to all university system resources. All Users are responsible for adhering to this policy.

III. Definitions

Capitalized terms shall have the meaning ascribed to them herein and shall have the same meaning when used in the singular or plural form or any appropriate tense.

- a. **Account:** An established relationship between a User and a computer, network, or Information System which is assigned a credential such as a username and password.
- b. **System Administrative Account:** An Account with elevated privileges intended to be used only when performing management tasks, such as installing updates and application software, managing user accounts, and modifying operating system and application settings.
- c. **Entitled Account:** A user who has met the minimum requirement to be granted authorization to access electronic Fairleigh Dickinson University Resources.

- d. **Authorized User:** A User who has been granted authorization to access electronic Fairleigh Dickinson University Resources and is current and active in their privileges.
- e. **Contractor or Vendor:** A person or a company that undertakes a contract to provide materials or labor to perform a service.
- f. **Employee:** University staff faculty and adjunct, including nonexempt, exempt, and overseas staff and collegiate faculty.
- g. **Multi-Factor Authentication (MFA):** Authentication using two or more different factors to achieve authentication. Factors include something you know (e.g., PIN, password); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric).
- h. **Privileged Account:** An Account that is authorized to perform security-relevant functions that an ordinary Account is not authorized to perform.
- i. **Single Sign-On (SSO):** An authentication process that allows an Authorized User to access multiple applications with one set of login credentials. SSO is a common procedure in enterprises, where a client accesses multiple resources connected to a local area network (LAN).
- j. **User:** A member of the University community, including but not limited to Staff and Faculty, and other individuals performing services on behalf of University, including Contractors, volunteers and other individuals who may have a need to access, use or control University Data.

IV. Authentication

- a. Any service, application or Information System, whether on-premise or in the cloud, that contains WISP protected information, especially PI or PHI; OR is accessed by a large group of employees (20 or more), must use Single Sign-on authentication.
 - i. If the service or application is being provisioned by a business unit, the unit must engage University Systems to work with the provider to enable SSO.
 - ii. If SSO is not supported by the service or application, it will not be approved for use by the university.
 - iii. See Section V for exceptions.

- b. Multi-factor authentication (MFA) must be used to access University resources.
- c. Passwords must be constructed in accordance with the minimum requirements as listed below:
 - i. Authorized User Account passwords must meet a minimum length of 8 characters.
 - ii. Administrative and Privileged Account passwords must meet a minimum of 10 characters.
 - iii. Passwords must contain a mix of alphanumeric characters. Passwords must not consist of all digits, all special characters, or all alphabetic characters.
 - iv. Automated controls must ensure that passwords are changed at 90-day intervals for both general users and administrative- level accounts.
 - v. NetIDs associated with a password must be disabled for a period of time after 10 consecutive failed login attempts. A minimum of 30 minutes is required for the reset period.
 - vi. Passwords must not be the same as the NetID.
 - vii. Passwords must not be displayed on screens.
 - viii. Users must not share passwords.
 - ix. Initial passwords and password resets must be issued pre-expired forcing the user to change the password upon first use.
 - x. Password reuse must be limited by not allowing the last 10 passwords to be reused. In addition, the password must be at least 2 days old in order to be voluntarily changed.
 - xi. Access will be disabled 90 days past the date that a password expired if not changed.
 - xii. Access will be disabled after 30 days of creation if NetID is not claimed.
 - xiii. Expired passwords must be changed before any other system activity is allowed.

V. **Server Password Protocol**

If, at any time, a member of the Community is granted permission to install a server, and access to that server is restricted via Login, and if that process is granted SSO exception through section VII., that system can not hold passwords in clear text. That system must use an approved irreversible cryptographic transform to protect its users' passwords.

VI. **Enforcement**

This policy will be enforced by technical controls wherever feasible; otherwise, this policy will be enforced by OIRT under the direction of the CIO. All members of FDU's faculty and staff have a responsibility to promptly report any known instances of noncompliance to AVP of University Systems and Networking or the Director of Systems.

Failure to comply with this policy can result in disciplinary action. Any such discipline shall be in accordance with processes and procedures of Human Resources and subject to any protections afforded under the University's agreement with "Office & Professional Employees International Union", the "Faculty Handbook", and similar documents. Third parties who violate this Policy may have their relationship with the University terminated and their access to campus restricted.

VII. **Exceptions**

Exceptions to this policy should be submitted to the AVP, USAN for review. Approval of the Chief Information Officer (CIO) or Data Security Incident Response Team (DSIRT) may be required.