Procedure 140-06 Password Complexity and Expiration

Sponsor: information Technology Services

Purpose

The purpose of this procedure is to protect institutional data and individuals whose data and/or security access may be comprised without adequate information technology security measures through the use of adequate password complexity and expiration.

Definitions

Critical system technical systems that are used to conduct financial operations, including Financial Aid, and house sensitive information.

High-value logins users granted advanced and administrative access with their credentials. This is usually IT staff.

MFA (Multifactor Authentication) the use of a second, or more, form of authentication, such as entering a text code or approving a message on an app.

Procedure

Passwords for all Network user accounts must meet the following minimum complexity requirements:

1. Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters.
2. Passwords must be at least 10 characters in length
3. Passwords must contain characters from at least three of the following four categories:
    a. English uppercase alphabet characters (A–Z)
    b. English lowercase alphabet characters (a–z)
    c. Base 10 digits (0–9)
    d. Non-alphanumeric characters (for example, !$#,%)
4. Multifactor (MFA) authentication is required for critical systems users and high-value logins.

Enforce Password History – X (cannot be published)

This setting determines the number of unique new passwords that have to be associated with a user account before an old password can be reused.

Maximum Password Age – X (cannot be published)

This setting determines the period of time (in days) that a password can be used before the system requires the user to change it.

Minimum Password Age – X (cannot be published)

This setting determines the number of days that must pass before a user can change his or her password. Defining a minimum password age prevents users from circumventing the password history policy by defining multiple passwords in rapid succession until they can use their old password again.

Student Initial Password – X (cannot be published)

References
March 2, 2022 Guidance on Multi Factor Authentication from the Arizona Auditor General
16 CFR § Part 314

Procedure History

05/18/2016	New and Approved by College Council
04/07/2022	Updated to reference guidance on multifactor authentication from Arizona Auditor General on multifactor authentication

Legal Review
None