Effective: *08/08/2022*
Last Revised: *03/12/2024*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Standard Contact:
IT Security Services

4.1.5 Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC)

The University should ensure that only authorized users have access to information systems. Access to networks, systems, and data should be role- or attribute-based where possible to ensure that permissions are assigned to end users in a consistent and uniform fashion ba

University is less vulnerable to information security attacks if permissions are granted to privileged users.

4.1.6 Portable Storage, Mobile Devices, and Mobile Computing Platforms

The University must limit the use of portable storage and mobile devices and at minimum, encrypt all High-Risk data on portable storage devices, mobile devices, and mobile computing platforms. Access controls must adhere to the **Media and Protection**

4.2.4 Multi-factor Authentication

All users must supply two forms of authentication (something they know, have, or who they are) when accessing University network or systems from university owned and issued endpoints. Second forms of authentication, such as

4.3 Privileged Access Management

4.4.2 Remote Access Authorizations

External access to internal information system resources utilizing the approved access mechanisms must only be granted to authorized University users.

Remote access to the environment by contractors, third-parties, vendors, or business partners must adhere to the authorization requirements defined in this Standard, must only be activated when needed, and must be immediately deactivated after use.

4.4.3 Multi-factor Authentication for Remote Access

4.6.3 Replay Resistant

For all network access of privileged and non-privileged accounts, authentication sessions between the authenticating client and the application server validating the user credentials must not be vulnerable to a replay attack.

4.6.4 Identifier Management

The University must manage user and system identifiers by:

- Establishing credentials that uniquely identify each user accessing an information system
- Verifying the identity of each user at login
- Receiving authorization to issue a user identifier is received from an appropriate member of management or other organization official and in accordance with policy and procedures.
- Ensuring that the user identifier is issued to the intended party or device identifier to the intended device in accordance with policy and procedures.
- Disabling the user identifier within 24 hours when the termination is mutual. In case of non-voluntary separation, the user identifier is disabled immediately
- Reviewing the user identifier when a user is transferred
- Disabling the employee user identifier after two years of inactivity
- Disabling the student user identifier after 365 days of inactivity; and
- Prohibiting the reassignment of user identifiers for a minimum of 365 days

4.7 Passwords Requirements

4.7.1 Password-based Authentication Control

Access to networks, information systems, and data must be regulated by authentication controls to restrict access to authorized users only. All password-