

Policy: Account Management

Purpose:

To provide a comprehensive account management process allowing only authorized individuals access to University Data and Information Systems.

Scope:

This policy applies to all Information Systems, University Data, identities and accounts used to access them and University Data.

Policy:

- 1. All persons and processes granted access to an information system, beyond that explicitly intended for unauthenticated public access must be uniquely and individually identified and authenticated.
- 2. All persons and processes that have been granted access to an information system must have an approved and documented level and scope of access.
- 3. Access to University Data and Information Systems is to be promptly modified upon changes in university affiliation, position, or responsibilities.

Responsibilities:

- 1. All members of the University Constituency are responsible for all actions initiated from accounts issued to them.
- Information Security Administrators (ISAs) are responsible for developing and implementing procedures to properly authorize, modify or terminate accounts and permissions.
- 3. Information Security Managers (ISMs) are responsible for implementing Information Systems such that account authorizations are promptly enforced.

Policy Number: Policy Family: Category:
SEC-XX-nnn Information Security Access Control

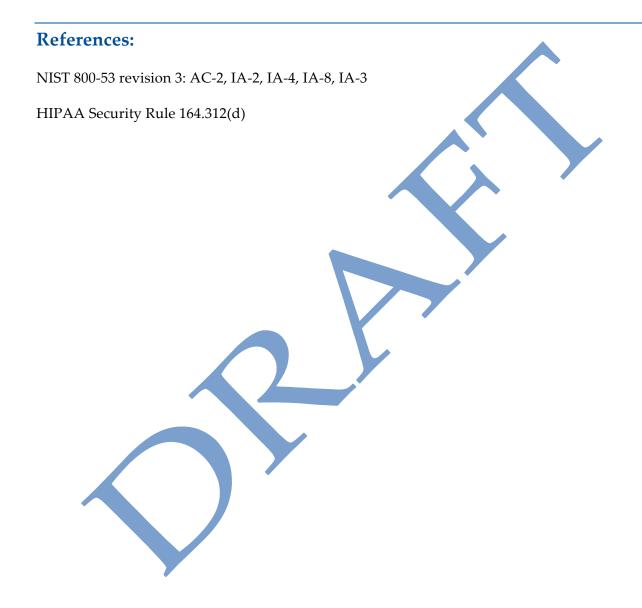
Effective Date: x/xx/201x

Policy: Account Management



Authority:

UF-1.0102: Policies on Information Technology and Security



Policy Number: SEC-XX-nnn

Policy Family: Information Security Category:
Access Control

Effective Date: x/xx/201x