UF UNIVERSITY of FLORIDA
Information Technology

Policy: Account Management

Purpose:

To provide a comprehensive account management process that allows 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.
2. Managers of university employees are responsible for promptly coordinating suspension of accounts for terminated employees.
3. Information Security Administrators (ISAs) are responsible for developing and implementing procedures to properly authorize, modify or terminate accounts and permissions.
4. Information Security Managers (ISMs) are responsible for implementing Information Systems such that account authorizations are promptly enforced.

Authority:

UF-1.0102: Policies on Information Technology and Security

References:

NIST 800-53 revision 3: AC-2, IA-2, IA-4, IA-8, IA-3

HIPAA Security Rule 164.312(d)

SEC-AC-001.01 Account Management Standard