Policy: TS0005	Category: Technical Security	Version Date: 11/19/2004
Title: User Account and Password Management		Effective Date: 3/31/2005
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review:
Review Resp: HSC Chief, Information Security		Next Review:

Purpose:

To ensure that access to electronic information assets is effectively managed by requiring that unique user account IDs and strong passwords are established for all networks and systems; that passwords are properly protected; and that passwords are changed periodically.

Scope:

This policy applies to all individuals and UF HSC Units that have been granted access to any information asset of the UF HSC Information and Computing Environment, including, but not limited to UF HSC faculty and staff, volunteers, students, and third parties.

References:

1. GatorLink Password Management Policy, http://www.it.ufl.edu/policies/passwords.html.
2. Standard GP0003.02: Information Classification.
3. Standard TS0005.02: User Accounts and Passwords

Policy:

1. All users of networks, systems, or applications must be supplied with a unique user account ID and a password, or other individually identifiable authentication method, to gain access to such systems to protect from unauthorized use. Each Unit must develop and implement written procedures for creating, changing, terminating and safeguarding the authentication method and, if user accounts and passwords are used, must comply with Standard TS0003: User Account and Password Management.
2. The registered user of an account that provides access to an information asset is responsible and liable for all processes initiated from that account. Unacceptable use, whether intentional or unintentional, will result in immediate suspension of the account.
3. Information access authority to Restricted or Sensitive information assets for each user or user group must be reviewed periodically (at least annually) for

CONFIDENTIAL – DO NOT RELEASE.
Exempt from disclosure pursuant to Section 119.071, Florida Statutes

appropriateness and the review documented at the direction of the Unit Information Security Administrator in conjunction with the owner's designee or delegate of the data or when an employee's job status changes.

4. Managers of networks, systems, or applications are responsible for making all users of their information assets aware of the latest password-related policies and procedures, the users' responsibilities under these procedures, and monitoring compliance with these procedures.
5. Security tokens must be returned on demand or upon termination of the relationship with the HSC or its affiliates.
6. If the confidentiality of a password is in doubt, the password must be changed immediately or the account disabled.