
Purpose:

Authentication mechanisms such as passwords are the primary means of protecting access to computer systems and data. It is essential that these authenticators be strongly constructed and used in a manner that prevents their compromise.

Scope:

This policy applies to all passwords and other authentication methods used at the university.

Policy:

1. Access to all university data and systems not intended for unrestricted public access requires authentication.
2. Passwords and other authenticators must be constructed to have a resistance to attack commensurate with the level of system or data access granted to the account.
3. Systems must be designed and configured to protect passwords during storage and transmission.
4. No one may require another to share the password to an individually assigned university account, for example as a condition of employment or in order to provide technical support.

Responsibilities:

1. All members of the University of Florida Constituency are responsible for any activity that occurs as a result of the use of authentication methods issued to them.
2. All members of the University of Florida Constituency are responsible for protecting the password or authentication method associated with an individually assigned university account. Passwords may not be shared or disclosed to anyone else.
3. All members of the University of Florida Constituency are responsible for reporting any suspicious use of assigned authentication mechanisms. Anyone that reasonably believes his

Policy: Authentication Management



or her password to be known by anyone else must change it immediately. Lost or stolen authentication devices are to be reported immediately.

4. Information Security Managers (ISM) are responsible for verifying that information systems under their control, and those intended for acquisition or development by their unit, comply with this policy.
5. The Vice President and Chief Information Officer is responsible for implementing systems and specifications to facilitate unit compliance with this policy.

Authority:

UF-1.0102: Policies on Information Technology and Security

References:

NIST 800-53 revision 3: AC-7, IA-5, IA-5 (1), IA-7

SEC-AC-002.01: Authentication Management Standard

SEC-AC-002.02: Password Complexity Standard

Policy Number: SEC-AC-002	Policy Family: Information Security	Category: Policy Category	Effective Date: 6/26/2013
-------------------------------------	---	-------------------------------------	-------------------------------------