UF UNIVERSITY of FLORIDA
Information Technology

Standard: Authentication Management

Purpose:

To establish minimum requirements for the secure use and storage of authentication mechanisms, such as passwords and 2-factor devices.

Standard:

1. Accounts are assigned to one of the following levels of password policy, based upon an individual or account's security roles(s), level of system access or classification of data to which the account grants access.

   P1 : **Entry**. Accounts providing access to basic university services, such as the campus network, but no access to Sensitive or Restricted data.

   P2 : **Low**. Accounts providing access to information only about oneself, no access to other Sensitive or Restricted data.

   P3 : **Medium**. Accounts providing access to information about others, provide data at unit level, access to Sensitive data and limited amounts of Restricted data.

   P4 : **High**. Accounts providing access to information at the institutional level, access to Restricted data (including Protected Health Information), privileged access to a system not containing Restricted data.

   P5 : **Rigorous**. Accounts providing access to control institutional systems, privileged access to a system containing Restricted data.

2. Each person affiliated with UF has one or more security roles; levels of system access; or access to data with different classification, each with varying password policies. If an individual has several roles, with conflicting levels of password policy, the "strongest" policy applies.

3. Upon creation or reset of an account, the system should prompt the user to create an initial password that complies with the Password Complexity Standard. In cases where this is not possible, the initial password must be unique, comply with the Password Complexity Standard, and require that the user change the password upon the first use.

4. Default passwords included as a part of any system must be changed as soon as practical, and in all cases prior to the system being placed into production use.

5. Passwords must never be stored in cleartext. Stored passwords above P3 should, whenever possible, be salted and hashed using encryption mechanisms intended for passwords, such as bcrypt or PBKDF2.

6. Transmission of passwords over any network must be encrypted.

7. All systems utilizing passwords must enforce the following requirements:

    a. Passwords must comply with the Password Complexity Standard.

    b. All users must read the Acceptable Use Policy before creating or changing a password.

    c. Users are advised in advance of password expiration, typically 14 days.

    d. Passwords with levels P1-P4 may be reset over the phone or using an online mechanism, once identity is verified using non-public information.

    e. Passwords with level P5 may only be reset in person, and upon physical verification of identity.

    f. Users with passwords of levels P4-P5 must pass a quiz at least once per year, demonstrating knowledge of password security requirements.

8. Passwords that can be independently discovered via internal testing, shared or publically disclosed shall be expired immediately.

9. The passwords to system and service accounts essential to the operation of an information system must be known or accessible to more than a single person. Such passwords must meet the requirements for level P5, be stored in a secure manner, and changed on a schedule relative to the risk of exposure and at a minimum when those with knowledge of the password terminate or are re-assigned.

References:

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

http://en.wikipedia.org/wiki/Bcrypt

http://en.wikipedia.org/wiki/PBKDF2