IT STD 1-01

Office of Information Technology
Technical Standard / Procedure

Security: Authentication / Passwords

Description:
Information is an asset that must be protected from unauthorized access, modification and destruction. The use of passwords is one method to provide protection by controlling access to information technology systems.

Standard:

- Agencies shall establish and implement criteria governing the following:
  - A reasonable number (3-5) of unsuccessful login attempts allowed prior to revocation of password.
  - Procedures for revoking and resetting passwords including a method to verify the identity of the person requesting the action.
  - Procedures for password length shall be established with particular attention paid to data classification and job function. The maximum validity period for passwords shall be:
    - 35 days with password length minimum of (8); or
    - 70 days with password length minimum of (10); or
    - 105 days with password length minimum of (12); or
    - 180 days with password length minimum of (15).

    NOTE: *Specific exemptions **MAY** be granted for special purposes (e.g. enabling a stored procedure to run against a database)*
  - Password re-use limitations.

- Use of passwords shall conform to the following requirements:
  - Passwords shall be kept confidential.
  - Categories of password complexity shall contain at least 3 of the 4 categories: English upper case characters (A-Z), English lower case characters (a-z), Base 10 digits (0-9), and non-alphanumeric characters (e.g., %, &, !).
  - Passwords shall not be kept on paper or stored in plain text format.
  - All passwords shall be changed whenever it is determined that a system's security may have been compromised.
  - The cycling or re-use of passwords shall be reasonably limited. Applicable devices and application systems shall maintain a password history file to prevent continual re-use of the same passwords or group of passwords for a valid user-ID (with 3 being the minimum number of previous passwords checked), where the capability exists.
  - Passwords must not be hard coded into software.
  - Passwords must not be stored in dial-up communications utilities or browsers.

Office of Information Technology
Technical Standard / Procedure

- Passwords must not be recorded in a system log unless the password is encrypted.
- Passwords must not be stored in any file, program, command list, procedure, macro, script or function key where it is susceptible to disclosure or to automate the login process.
- Temporary or "reset" passwords shall be changed upon first use.
- After a reasonable number (3-5) of consecutive failed attempts at log in, the user-ID shall be marked inactive and require a reset before additional log in attempts are allowed.
- All default passwords must be deleted or changed immediately upon first use.
- If not done at the time of creation, all passwords shall be checked periodically (annually or more often) via automated tools for weaknesses and to ensure that they conform to all proscribed rules for passwords, where such capability exists.
- When changing a password, the user must provide the old password before a new password can be created, where such capability exists.

- Self-Service Password Reset – Whether developed in-house or purchased as a third-party option, tools that enable end-users to reset their passwords must conform to the following criteria:
  - Questions must be asked to confirm the identity of the person requesting a password reset. The questions used shall not be ones to which the answers would conflict with privacy legislation, policies or would be commonly known to another (e.g., mother's maiden name is fairly trivial information for an attacker to determine). The user should be able to provide the questions and answers to be asked at the time the user-ID and password are initially created.
  - There shall be a reasonable number of times (3-5) a user can enter an incorrect answer.
  - The tool must provide for secure encrypted storage of the questions and answers.

Transition:
All newly deployed systems and applications must be compliant with this standard. Where possible existing systems and applications should be modified to become compliant with this standard. However, those systems requiring extensive modifications are exempt from this standard. Exemptions to this standard should be submitted in writing to the Chief Information Security Officer where the document will be kept on file.

Procurement:
Not applicable.

Related Policies, Standards, Guidelines:

Office of Information Technology
Technical Standard / Procedure

- Intrusion detection software should be used where applicable to deter unauthorized attempts at guessing passwords.
- Authentication software should allow for the changing of a password by the user/customer at will and without outside help.
- Most systems will "reset" the number of consecutive failed attempts to zero after each successful entry or once per day (usually late at night). This "reset" should not be done for accounts for which the threshold has been exceeded. For example, if the threshold is set for 5-consecutive attempts, then accounts having reached this number and placed into a "locked" or "disabled" state should remain in this state and not be reset without manual intervention, whether done by an Administrator or through the Self-Service Password Reset.
- Passwords should be stored and transmitted as encrypted data.
- Wherever possible, self-help password resetting tools should be employed to reduce the support workload.

Owner:
OIT Security Office

Effective Date:
July 27, 2009