AUTHENTICATION POLICY

June 2007 TNS –POL - 009

Purpose:
Access to data or resources in a computer system with the most basic level of security most often requires the user to identify himself and prove his identity. The user's identification (user-ID) tells the system who the user is and the user's password proves, or authenticates, the user's identity. Once the system knows who the user is, it can determine what data and resources the user can access.

Authentication focuses on something you know (passwords, PIN), something you have (digital tokens, smart cards) and something you are (biometrics). Any combination of these can be used to authenticate a user. Most computer systems rely on a user-ID and password for authentication. However, authentication can be much more secure when these methods are combined.

Information is a university asset that must be protected from unauthorized access, use, modification and destruction. The authentication process provides protection by controlling access to the assets of information technology systems. Authentication techniques permit validation of user's identities, hardware devices, and/or transmitted information.

Policy:
University departments must use at least use one of the following methods of authentication when accessing or utilizing university-owned or managed information technology systems.

- Passwords
- Biometrics
- Smart Cards
- PKI

Scope:
All colleges and departments under the authority of the Office of Technology and Network Services (TNS) must comply with this policy.

Responsibilities:
Technology and Network Services is responsible for developing policies governing the authentication requirements detailed in this policy and its supporting technical standards.

Effective Date:
June 20, 2007

Authentication / Passwords

Definition(s):
Authentication is the verification of the identity of a person or process. A password is a secret series of characters that, by association with a user-ID, allows access to information, systems, applications, or networks.

Rationale:
Information is a state asset that must be protected from unauthorized access, modification and destruction. Passwords are one method to provide protection by controlling access to information technology systems.

Approved Standards:
Agencies shall establish and implement criteria governing the following:

- A reasonable number three (3) 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.
- Maximum validity periods for passwords to be no greater than 30 days, with specific exemptions granted for special purposes such as 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.
- Minimum password length and format shall be no less than eight (8) characters.
- Minimum password complexity should 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 (%,&,!).
- 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.
- Passwords shall be changed on a monthly basis and the cycling or re-use of passwords will be reasonably limited. Applicable devices and application systems shall maintain a password history file to prevent continual reuse 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.
- 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 log in process.
- Temporary or "reset" passwords shall be changed upon first use.
- After a reasonable number three (3) of consecutive failed attempts at log in, the user-ID shall be marked inactive and require a reset before additional log in attempts are possible.
- All default passwords must be deleted or changed immediately upon first use.
- If not done at the time of creation, all passwords must 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 exist.

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 should 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 should be a reasonable number of times three (3) a user can enter an incorrect answer.
- The tool must provide for secure encrypted storage of the questions and answers.

Approved Products:
This is a functional standard for any implementation of passwords.

Guidelines/Technical Considerations:

- 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.
- Passwords should be stored and transmitted only as encrypted data.
- Temporary, initial, or "reset" passwords should be randomly generated, unique, and lock out the user-ID account if not changed after a short period of time (maximum of 5 minutes). Many password security systems use the same default password for all resets and new user-IDs and do not require the user to sign on immediately to change the password.
- Wherever possible, self-help password resetting tools should be employed to reduce the support workload.

Review Cycle:
As needed.

Timeline:
Issued: June 20, 2007

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.