SUnet PASSWORD POLICY

July 2007 TNS –POL - 010

Purpose

Information is a university 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.

Scope

The policy applies to all Southern University Baton Rouge (SUBR) users: students, faculty, staff, administrators, systems, applications and networks.

Definition

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.

Policy and Procedures

IT Security Services have established and implemented this criterion governing the following:

- A reasonable number (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.
- Maximum validity periods for passwords to be no greater than 60 days, with specific exemptions granted for special purposes such as enabling a stored procedure to run against a database.
- Passwords re-use limitations (5 times).

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 2 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 regular 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 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 (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 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 (5) a user can enter an incorrect answer.
- The tool must provide for secure encrypted storage of the questions and answers.

Help Desk Assisted Password Reset – The user can visit the Office of Technology and Network Services for assistance with password reset.

- User must appear in person.
- User must present University photo identification.
- User may be required to present secondary photo identification.
- User must change password upon first login after reset.

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.
- The self-help password resetting tools should be employed to reduce the support workload.

Policy Approval:
Effective August, 15, 2007