PASSWORD POLICY

Policy Statement

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Southern Miss's entire corporate network. As such, all Southern Miss employees (including contractors and vendors with access to Southern Miss systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Reason for Policy/Purpose

This policy is required for the effective communication of university policies regarding the standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Who Needs to Know This Policy

All personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Southern Miss facility, has access to the Southern Miss network, or stores any non-public Southern Miss information.

Website Address for this Policy

www.usm.edu/institutional-policies/policy-acaf-it-015

Definitions

Application Administration Account
Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).
1.0 GENERAL

1.1 All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

1.2 All production system-level passwords must be part of the Information Security administered global password management database.

1.3 All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.

1.4 User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.

1.5 Passwords must not be inserted into email messages or other forms of electronic communication.

1.6 Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

1.7 All user-level and system-level passwords must conform to the guidelines described below.

2.0 GENERAL PASSWORD CONSTRUCTION GUIDELINES

Passwords are used for various purposes at Southern Miss. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

2.1 Strong passwords have the following characteristics:
Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+-\[\]":;'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase.

For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

2.2 Poor, weak passwords have the following characteristics:
- The password contains less than eight characters.
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

NOTE: Do not use either of these examples as passwords!

3.0 PASSWORD PROTECTION STANDARDS

3.1 Do not use the same password for Southern Miss accounts as for other non-Southern Miss access (e.g., personal ISP account, option trading, benefits, etc.).

3.2 Where possible, don't use the same password for various Southern Miss access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

3.3 Do not share Southern Miss passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Southern Miss information.

3.4 Don’t:
- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- If someone demands a password, refer them to this document or have them call someone in the Information Security Department.
- Avoid using the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).
- Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

3.5 Do:
- Change passwords at least once every 6 months.
- System-level passwords used by System Administrators must be changed quarterly.
- If an account or password is suspected to have been compromised, report the incident to Information Security and change all passwords.

3.6 Password cracking or guessing may be performed on a periodic or random basis by Information Security or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

4.0 APPLICATION DEVELOPMENT STANDARDS

Application developers must ensure their programs contain the following security precautions.

4.1 Applications:
- must support authentication of individual users, not groups.
- must not store passwords in clear text or in any easily reversible form.
- must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible. (Definition Section 6.0)

5.0 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**Review**

The Chief Information Officer is responsible for the review of this policy every four years (or whenever circumstances require immediate review).

**Forms/Instructions**
Appendices

N/A

Related Information

N/A

History

1. 11/16/06: Outline structure modified slightly to accommodate HTML format.
2. 11/16/06: Posted to website.
3. 04/23/08: Modified policies menu.
4. 11/01/11: Formatted for Institutional Policies website.
5. 02/19/13: Formatted for template. Policy section renumbered. Minor editing of punctuation and usage throughout.

Amendments: Month, Day, Year – summary of changes
Authorization

PASSWORD POLICY
ACAF-IT-015

As the Responsible Officer, I have reviewed this policy and believe it represents the current policy.

[Signature]
Responsible Officer

[Signature]
Date
4/30/13