# Password Guidelines

## Purpose

Passwords are a critical part of information and network security. Passwords serve to protect user accounts, but a poorly chosen password, if compromised, could put the entire network at risk. As a result, all employees of Texas Southmost College are required to take appropriate steps to ensure that they create strong, secure passwords and keep them safeguarded at all times.

The purpose of this guideline is to set a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected.

## Scope

This guideline applies to all faculty and staffs of Texas Southmost College who have or are responsible for a computer account, or any form of access that supports or requires a password, on any system that resides at any Texas Southmost College facility, has access to the Texas Southmost College network, or stores any non-public Texas Southmost College information.

## Guideline

### General

1. Passwords must be changed every 120 days.
2. Old passwords cannot be re-used for a period of 12 months.
3. Users will be notified two weeks in advance of password expiration date. At this time, users will be prompted to select a new password.
4. All passwords must conform to the guidelines outlined below.

### Password Construction Guidelines

Passwords are used to access any number of institutional systems, including the network, e-mail, administrative/education systems, library systems, and voicemail. Poor, weak passwords are easily cracked, and put the entire system at risk. Therefore, strong passwords are required. Try to create a password that is also easy to remember.

1. Passwords should not be based on well-known or easily accessible personal information.
2. Passwords must contain at least eight characters.
3. Passwords must contain at least one uppercase letter(s) (e.g. N) and six lowercase letters (e.g. t).
4. Passwords must contain at least one numerical character (e.g. 5).
5. A new password must contain at least two characters that are different than those found in the old password which it is replacing.

6. Passwords must not be based on a users' personal information or that of his or her friends, family members, or pets. Personal information includes logon I.D., name, birthday, address, phone number, social security number, or any permutations thereof.

7. Passwords must not be words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon.

8. Passwords must not be based on publicly known fictional characters from books, films, and so on.

9. Passwords must not be based on the college's name or geographic location.

## Password Protection Guidelines

1. Passwords should be treated as confidential information. No employee is to give, tell, or hint at their password to another person, including IT staff, administrators, superiors, other co-workers, friends, and family members, under any circumstances.

2. If someone demands your password, refer them to this guideline or have them contact the IT Help Desk.

3. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to institutional resources via the college's IPsec-secured Virtual Private Network or SSL-protected Web site.

4. No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.

5. Do not use the "Remember Password" feature of applications or web services.

6. Passwords used to gain access to institutional systems should not be used as passwords to access non-institutional accounts or information.

7. If an employee either knows or suspects that his/her password has been compromised, it must be reported to the IT Help Desk and the password changed immediately.

_____