SOUTHWEST TENNESSEE COMMUNITY COLLEGE

SUBJECT: Electronic Information Security Policy

EFFECTIVE DATE: September 1, 2007 ;Rev. : January 21, 2010; Rev. January 21, 2015

The Electronic Information Security Policy will be consistent with and not supersede other Southwest Tennessee Community College policies, including the Information System "Acceptable Usage Policy."

A. General

1. The purpose of this policy is to set minimum standards for access to, and control and security of, electronic information. As much as any physical resource of the college, electronic information is a vital asset, and its security must be ensured in order to prevent theft, fraud, or other misuse of data.

2. The scope of this policy includes all personnel who have or are responsible for electronic information on any system that resides at any Southwest facility, has access to the Southwest network, or stores any Southwest information.

B. Password Security

1. 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 Southwest's entire enterprise network. As such, all Southwest employees (including contractors and vendors with access to Southwest systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Source of Policy: Information Technology
Responsible Administrator: Executive Director, Information Services
TBR Policy Reference: N/A
Related Policy: N/A
TBR Guideline Reference: N/A

Approved: _____ **President**
Date: June 1, 2015

2. General

a. All system-level passwords (e.g., root, enable, system administration accounts, etc.) must be changed on at least a 100-day basis.
b. All application administration account passwords (e.g. accounts which control application processes) must be changed on at least a 150-day basis.
c. All user-level passwords (e.g., network log-in, ERP, etc.) must be changed at least every 150-days. Password policies for desktop, web, or email may be implemented at the discretion of the Southwest.
d. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
e. Passwords must not be inserted into email messages or other forms of electronic communication.
f. All user-level and system-level password construction must conform to the guidelines for strong passwords described in the general guidelines for password construction and protection, applications development and passphrases located at: http://www.southwest.tn.edu/documents/infosys/passwordguidelines.pdf
g. A history of the past 10 passwords will be kept to prevent users from reusing them.
h. The minimum age duration for passwords will be one day.
i. The password “grace period” will be set to 10 days during which the user will be warned that the password is due to expire.
j. Accounts will be locked after five invalid password attempts.
k. The lockout attempts counter will be reset after 30 minutes.
l. The account will be locked out for 30 minutes if the account is locked due to invalid password attempts.
m. The account or computer will automatically lock or log off if it has remained inactive for a period of 20 minutes.
n. These password control settings apply to all accounts (e.g. network, web, application, Oracle) as best as they can be implemented.
o. Proper protection of password standards including guidelines relating to applications development, are described in the guidelines located at: http://www.southwest.tn.edu/documents/infosys/passwordguidelines.pdf

3. Use of Passwords and Passphrases for Remote Access Users

Access to the Southwest networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase. Guidelines for passphrases are described at: http://www.southwest.tn.edu/documents/infosys/passwordguidelines.pdf

C. Confidentiality of Personally Identifiable Information.

Clients will never be asked for your personally identifiable information including your username and password for College information technology systems.

Do not share Southwest passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Southwest information. You will never be asked to provide personally identifiable information regarding your College information systems access.

D. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

All users of Southwest Tennessee Community College computer and telecommunications resources are expected to read and abide with the college's Acceptable Computer Usage Policy.