SOUTHWEST TENNESSEE COMMUNITY COLLEGE

SUBJECT: Electronic Information Security

EFFECTIVE DATE: September 1, 2007; Revised January 21, 2010; Revised January 21, 2015; Revised July 1, 2024

*In October of each year, Information Technology related policies are reviewed as required by external regulations.

Purpose

The purpose of this policy is to set minimum standards for access to, control of, and security of, electronic information collected by Southwest Tennessee Community College ("Southwest" or "the College") through the use of passwords.

Definitions

Authentication- A process that allows a device or system to verify the unique identity of a person, device, or other system that is requesting access to a resource.

Digital Identity- Information on an entity used by computer systems to represent an external agent. That agent may be a person, organization, application, or device. Also referred to as a user account or user profile.

System Account- A special account used for automated processes without user interaction or for device management. These accounts are not assigned to an individual user for login purposes.

Privileged Account- An account with elevated access or privileges to a secure system or resource. This type of account is authorized and trusted to perform security relevant functions that an ordinary user account is not authorized to perform. Privileged accounts are assigned to individual users.

Personally Identifiable Information (PII)- Information which can be used to distinguish or trace an individual's identity, such as their ID, social security number, or biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Policy

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.

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.

This policy is intended to be consistent with and not supersede other Southwest policies, including the Acceptable Usage policy, 6:00:00:00/5.

Southwest shall control user access to information assets based on requirements of individual accountability, need to know, and least privilege.

College information access must be authorized and managed securely in compliance with appropriate industry practice and with numerous applicable legal and regulatory requirements (e.g., HIPA, FERPA, the Open Records Act, etc.).

College information assets include data, hardware, and software technologies, and the infrastructure used to process, transmit, and store information.

A. Any computer, laptop, printer, or device that an authorized user connects to the campus network is subject to this policy.

B. Guest, unauthenticated access may be provisioned commensurate with usage and risk.

C. Authorized users accessing College computing resources and network with their own personal equipment are responsible for ensuring the security and integrity of the systems they are using to establish access.

For systems that contain critical or confidential classified data, Southwest will use secure methods that uniquely identify and authenticate users. Such methods can include multi-factor authentication, passwords, data loss prevention, device management, biometrics, and public/private key pairs.

Access Controls

A. Access to information assets must be restricted to authorized users and must be protected by appropriate physical, administrative, and logical authentication and authorization controls.

B. Protection for information assets must be commensurate with the classification level assigned to the College by the Tennessee Board of Regents ("TBR").

C. Each computer system will have an automated access control process that identifies and authenticates users and then permits access based on defined requirements or permissions for the user or user type.

D. All users of secure systems must be accurately identified, a positive identification must be maintained throughout the login session, and actions must be linked to specific users.

E. Access control mechanisms may include user IDs, access control lists, constrained user interfaces, encryption, port protection devices, secure gateways/firewalls, and host-based authentication.

User Identification, Authentication, and Accountability

A. User IDs
   1. Each user must be identified through a unique user identifier (user ID) account.
   2. User IDs are assigned by Information Technology Services and application support personnel.

3. Users must provide government-issued, picture IDs for positive proof of identity when receiving account access.
4. Users must provide their user ID at logon to a computer system, application, or network.

B. Individual Accountability
1. Individual accountability must be maintained.
2. Each user ID must be associated with an individual person who is responsible for its use.
3. Individuals with authenticated access cannot share their login credentials with anyone with the penalty of having their access rescinded immediately.

C. Authentication
1. Authentication is the means of ensuring the validity of the user identification.
2. All user access must be authenticated.
   a. The minimum means of authentication is a personal secret password that the user must provide with each system and/or application logon.
   b. All passwords used to access information assets must conform to certain requirements relating to password composition, length, expiration, and confidentiality.

Password Security

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) and students are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

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 every 150-days. Password policies for desktop, web, or email may be implemented at the discretion of the College.

D. All temporary passwords (e.g. guest password and registration password) shall be changed on a 24-hour basis.

E. 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.

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

G. All user-level and system-level password construction must conform to the guidelines for password construction and protection, applications development, and passphrases located at: http://www.southwest.tn.edu/documents/infosys/passwordguidelines.pdf

H. A history of the past ten (10) passwords will be kept to prevent users from reusing them.

I. The minimum age duration for passwords will be one (1) day.

J. The password "grace period" will be set to ten (10) days, during which the user will be warned that the password is due to expire.

K. Accounts will be locked after five (5) invalid password attempts.

L. The lockout attempts counter will be reset after thirty (30) minutes during which time the account will be locked out.

M. The account or computer will automatically lock or log off if it has remained inactive for a length of time.

N. These password control settings apply to all accounts (e.g., network, web, application, etc.) as best as they can be implemented.

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

Confidentiality of Personally Identifiable Information

Clients will never be asked for personally identifiable information, including username or password.

Do not share Southwest passwords with anyone, including administrative assistance and secretaries. All passwords are to be treated as sensitive, confidential Southwest information. Users will never be asked to provide personally identifiable information regarding College Information Systems access.

Access Privileges

A. Each user's access privileges shall be authorized on a need-to-know basis as dictated by the user's specific and authorized role.

B. Authorized access shall be based on least privilege.

1. This means that only the minimum privileges required to fulfill the user's role shall be permitted.
2. Access privileges shall be defined to maintain appropriate segregation of duties to reduce the risk of misuse of information assets.
3. Any access that is granted to data must be authorized by the appropriate data trustee.

C. Access privileges shall be controlled based on the following criteria, as appropriate:

1. Identity (user ID);
2. Role or function;
3. Physical or logical locations;

4. Time of day/week/month;
5. Transaction based access;
6. Access modes such as read, write, execute, delete, create, and/or search.

D. Privileged access (e.g., administrative accounts, root accounts) must be granted based strictly on role requirements. The number of personnel with special privileges should be carefully limited.

Access Account Management

A. User ID accounts must be established, managed, and terminated to maintain the necessary level of data protection.

B. The following requirements apply to network logons as well as individual application and system logons, and should be implemented where technically and procedurally feasible:

1. Account creation requests must specify access either explicitly or request a role that has been mapped to the required access. New accounts created by mirroring existing user accounts must be audited against the explicit request or roles for appropriate access rights.

2. Information Technology personnel revoke access upon notification that access is no longer required in accordance with the following procedures:

a. Access privileges of terminated or transferred users must be revoked or changed as soon as notification of termination or transfer occurs.
b. In cases where an employee is not leaving on good terms, the user ID must be disabled simultaneously with departure.
c. Access for users who are on leaves of absence or extended disability must be suspended until the user returns.
d. Adjunct faculty members are never granted access to Banner Admin Pages.
e. Adjunct faculty member account access shall be controlled by the College's IT Services using contract status, defined dates of employment, and any data relevant to contract control for adjunct faculty.
f. Adjunct faculty members shall be granted limited access before and after their course start and end dates to perform the duties necessary for their position, upon request involving reasons for the extension and specific access.

3. User IDs will be disabled after a period of inactivity that is determined appropriate by the College.

4. All third-party access (contractors, business partners, consultants, vendors, etc.) must be authorized and monitored by the College.

5. A periodic audit of secured systems to confirm that access privileges are appropriate must be conducted.

a. The audit will consist of reviewing and validating that user access rights are still needed and are appropriate.

6. Applications requiring an account not tied to a single user shall employ service-based accounts.

a. Users oversee these accounts and maintain their passwords.
b. Applications requiring these accounts shall be monitored and audited by the College.
c. Service-based accounts, due to their application-centric use, are not subject to standard user account management rules.

Compliance and Enforcement

A. This policy applies to all users of College information resources including students, faculty, staff, temporary workers, vendors, and any other authorized users who are permitted access.

B. Any employee found to have violated this policy may be subject to disciplinary action (to be determined and enforced by the College), including the loss of computer network access privileges, disciplinary action, dismissal from the College, and legal action.

C. Some violations may constitute criminal offenses. The College will carry out its responsibility to report such violations to the appropriate authorities.

Exceptions

A. Documented exceptions to this policy may be granted by Information Technology Services based on limitations to risk and use.

All users of Southwest computer and telecommunications resources are expected to read and abide by the College's Acceptable Usage Policy, 6:00:00:00/5.

Source of Policy: Information Technology

Responsible Administrator: Chief of Administrative Services

Related Policy: 6:02:10:02/26; 6:00:00:00/23; 6:00:00:00/5; 6:00:00:00/22

TBR Policy Reference: 1.08.00.00; 1.08.03.00

Approved: _____
President

Date: July 1, 2024