HSCEP OP: 56.50 – Access Control (AC)

Policy Statement:

TTUHSC El Paso shall implement logical access controls to limit access to systems and process to authorized users.

Reason for Policy:

The purpose of the Access Control (AC) policy is to ensure that TTUHSC El Paso limits access to its systems and data to authorized users in accordance with TAC 2021, NIST 800-53 and other governing entities. Information resources are valuable assets to TTUHSC El Paso and regulating access promotes confidentiality, integrity, and accessibility of protected information resources.

Entities Affected by this Policy are any and all users of Information Resources at TTUHSC El Paso.

What is covered in this Policy?

The overall policy addresses the Institutional stance as it applies to TTUHSC El Paso in the areas of: account management, access enforcement, information flow enforcement, separation of duties, least privilege, login access and notifications, session control, remote and wireless access including mobile devices, information sharing, publicly accessible content, access control decisions and monitoring.

Access Control is a breakdown of who has access, to what, for how long, using what methods, under what permissions and authority, and how access is monitored. It is the stance of TTUHSC El Paso to ensure that there are safeguards in place aligned with NIST 800-53 and TAC 202 to ensure the protection, integrity, and confidentiality of information resources at TTUHSC El Paso.

Who Should Read this Policy?

All individuals accessing, storing, viewing any TTUHSC El Paso information resources.

What happens if I violate this policy?

Any person(s) violating TTUHSC El Paso Information Technology policies are subject to penalty under federal, state, and local legislation. Disciplinary actions are further outlined in HSCEP OP 56.50 Sanction Policy (SN)2.

AC-01: Access Control Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates:

- A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

TTUHSC El Paso is required to document organization-wide media protection controls that, at a minimum, include:

a. A formal, documented media protection policy; and
b. Processes to facilitate the implementation of the media protection policy, procedures and

associated controls.

MP-02: Account Management

The organization manages system accounts, including:

- Automated System Account Management - Where technically feasible, automated mechanisms are required to be configured to automatically alert appropriate personnel for security-related changes in account status.
- Removal of Temporary/Emergency Accounts - System automatically disables or removes temporary and emergency accounts after an organization-defined time period for each type of account.
- Disable Inactive Accounts - The information system automatically disables inactive accounts after an organization-defined time period.
- Automated Audit Actions - The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies organization-defined personnel or roles.
- Inactivity Logout - The organization requires that users log out after an organization-defined time period of expected inactivity. If a session has been idle for more than fifteen (15) minutes, the user must be logged out and required to re-authenticate to re-activate the session.
- Role-based Schemes (Role-Based Access Control (RBAC)) – TTUHSC El Paso establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles; monitors privileged role assignments; and takes actions when privileged role assignments are no longer appropriate.
- Restrictions on Shared Groups/Accounts - Only when justified by a valid business case, TTUHSC El Paso permits the use of shared/group accounts.
- Shared/Group Account Credential Termination - When members no longer need access to a shared/group account, data owners need to change permissions and access to a shared/group account, on all affected information systems in a timely manner.

The TTUHSC El Paso IT Department is required to:

- Identify account types (e.g., individual, group, system, application, guest/anonymous, and temporary);
- Establish conditions for group membership;
- Identify authorized users of the system and specify access privileges;
- Require appropriate approvals for requests to establish accounts;
- Establish, activate, modify, disable, and remove accounts;
- Specifically authorize and monitor the use of guest/anonymous and temporary accounts;
- Notify account managers when temporary accounts are no longer required and when system users are terminated, transferred, or system usage or need-to-know/need-to-share changes;
- Deactivate accounts that are no longer required;
- Grant access to the system based on a valid access authorization; and
- Review accounts on a regular basis.

TTUHSC El Paso's IT department is responsible for ensuring proper user identification and authentication management for all standard and privileged users on all systems, as follows:

- Control addition, deletion, and modification of user IDs, credentials, and other identifier objects to ensure authorized use is maintained;
- Verify user identity before issuing initial passwords or performing password resets;
- Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use;
- Immediately revoke access for any terminated users;
- Remove/disable inactive user accounts within ninety (90) days;
- Limit repeated access attempts by locking out the user ID after not more than six (6) attempts;
- Set the lockout duration to fifteen (15) minutes or until the administrator enables the user ID;

- Establish and administer accounts in accordance with a role-based access scheme that organizes system and network privileges into roles;
- Track and monitor role assignments for privileged user accounts;
- Automatically terminate access for temporary and emergency accounts after the accounts are no longer needed;
- Enable accounts used by vendors for remote access only during the time period needed and monitor vendor remote access accounts when in use;
- Minimize the use of group, shared, or generic accounts and passwords;
- Default user IDs and accounts are disabled or removed;
- Service providers with remote access to TTUHSC El Paso's premises (e.g., for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer; and
- Restrict user direct access or queries to databases to database administrators, including:
- Verify that database and application configuration settings ensure that all user access to, user queries of, and user actions on (e.g., move, copy, delete), the database are through programmatic methods only (e.g., through stored procedures);
- Verify that database and application configuration settings restrict user direct access or queries to databases to database administrators; and
- Review database applications and the related application IDs to verify that application IDs can only be used by the applications and not by individual users or other processes.

AC-03: Access Enforcement

TTUHSC El Paso is required to limit access to systems and sensitive data to only those individuals whose job requires such access.

AC-04: Information Flow Enforcement – Access Control Lists (ACLs)

Network administrators are required to enforce information flow control using:

a. Access Control Lists (ACL) as a basis for flow control decisions;
b. Documented business justification for the use if all services, protocols, and ports allowed;
c. Explicit security attributes on information, source, and destination objects as a basis for flow control decisions;
d. Demilitarized Zones (DMZ) are required to be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports; 5
e. Inbound Internet traffic shall be limited to IP addresses within the DMZ; 6
f. Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network; 7
g. Unauthorized outbound traffic to the Internet is prohibited; 8
h. Stateful inspection (dynamic packet filtering) must be implemented; 9
i. System components that store cardholder data must be placed within an internal network zone, segregated from the DMZ and other untrusted networks; 10 and
j. Private IP addresses and routing information are prohibited from being disclosed to unauthorized parties.

Information Flow Enforcement shall include:

Object Security Attributes

Data/process owners and asset custodians are required to use security attributes associated with information, source, and destination objects to enforce defined information flow control policies as a basis for flow control decisions.

Content Check For Encrypted Data

When necessary for business purposes, TTUHSC El Paso's IT security personnel are authorized to implement steps to block encrypted data that cannot be analyzed by content-checking

mechanisms.

Embedded Data Types

When necessary for business purposes, TTUHSC El Paso's IT security personnel are authorized to block embedded data types.

Metadata

When necessary for business purposes, TTUHSC El Paso's IT security personnel are authorized to implement steps to block data based on metadata tags as part of TTUHSC El Paso's Data Loss Prevention (DLP) program.

Human Reviews

TTUHSC El Paso IT Security is responsible for implementing a review of firewall and router rule sets at least once every six (6) months to ensure least privileges and best practices are being followed.

Physical / Logical Separation for Information Flows

Where technically feasible and justified by a valid business case, TTUHSC El Paso shall separate information flows logically or physically using mechanisms and/or techniques to accomplish separations by types of information.

AC-05: Separation of Duties

In sensitive environments, TTUHSC El Paso management is required to:

a. Separate duties of individuals, as necessary, to prevent malevolent activity without collusion;
b. Document any separation of duties; and
c. Where technically feasible, implement separation of duties through assigned system access authorizations.

AC-06: Least Privilege

TTUHSC El Paso follows the "principle of least privilege,"12 which states that only the minimum access necessary to perform an operation should be granted. Access will be granted only for the minimum:

a. Levels of permissions necessary to perform the job function; and
b. Time required.

Least Privilege includes:

Authorize Access to Security Functions

Only explicitly-authorized personnel are permitted to have access to security functions and security-related information.

Non-Privileged Access for Non-Security Functions

Users must use accounts with the least functionality necessary to perform their job functions and are therefore prohibited from using privileged accounts to perform non-privileged functions.

Privileged Accounts

Assignment of privileged accounts must be limited to users who have:

a. A valid business justification;
b. Received security awareness training commensurate with the level of risk from having privileged access; and
c. Demonstrated technical competence specific to the environment where privileged access is being granted.

Auditing Use of Privileged Functions

TTUHSC El Paso is required to establish a process for linking all access to systems, including administrative privileged accounts (e.g., root or administrator) to each individual user.

Prohibit Non-Privileged Users from Executing Privileged Functions
Where technically feasible, information systems must be configured to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

AC-07: Unsuccessful Login Attempts

TUHSC El Paso's IT department is required to configure:

a. Systems to automatically lock the accounts until released by an administrator when the maximum number of unsuccessful attempts is exceeded; and
b. The maximum number of consecutive, unsuccessful access attempts is six (6) attempts.
c. Where technically feasible, mobile devices are required to be configured to be automatically purged after no more than ten (10) consecutive, unsuccessful login attempts to the mobile device.

AC-08: System Use Notification (Logon Banner)

Systems will:

- Display an approved system use notification message or banner before granting access to the system that provides privacy and security notices; and
- Retain the notification message or banner on the screen until the user takes explicit actions to log in to or further access the system.

Banner will include language that states:

- Unauthorized use is prohibited;
- Usage may be subject to security testing and monitoring;
- Misuse is subject to criminal prosecution; and
- Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

AC-09: Previous Logon Notification

Asset custodians are required to configure systems that process, store or transmit sensitive data to notify the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

AC-10: Concurrent Session Control

TTUHSC El Paso requires that concurrent sessions are limited to users, based on the role of the account:

a. Users: Standard user accounts should be configured to have no more than two (2) concurrent sessions; and
b. Administrators: Privileged user accounts should be configured to have no more than five (5) concurrent sessions.

AC-11: Session Lock

TTUHSC El Paso Systems must:

a. Prevent further access to systems by initiating a session lock after fifteen (15) minutes of inactivity or upon receiving a request from a user; and

b. Retain the session lock until the user reestablishes access using established identification and authentication procedures.
c. Information systems must be configured to conceal, via the session lock, information previously visible on the display with a publicly viewable image.

AC-12: Session Termination

Systems are required to be configured to automatically log users off and require the user to re-authenticate to re-activate the terminal or session if a session has been idle for more than fifteen (15) minutes.

AC-13: Supervision & Review

TTUHSC El Paso requires asset custodians to:

a. Determine normal time-of-day and duration usage for system accounts;
b. Monitor for atypical usage of system accounts; and
c. Report of atypical usage in accordance with incident escalation procedures.

AC-14: Permitted Actions Without Identification or Authorization

TTUHSC El Paso prohibits system configurations that do not require identification or authentication, without a documented and justifiable business requirement.

AC-15: Automated Marking

TTUHSC El Paso marks, in accordance with organizational policies and procedures, system media and system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information to aide Data Loss Prevention (DLP) and Network Access Control (NAC). Asset custodians are required to configure systems to mark metadata in environments where Data Loss Prevention (DLP) and Network Access Control (NAC) technology is being used.

AC-16: Security Attributes

Systems support and maintain the binding of organization-defined security attributes to information in storage, process, and transmission.13 Systems are required to be configured to display security attributes in human-readable form on each object output

AC-17: Remote Access

TTUHSC El Paso's IT security personnel are responsible for:

a. Documenting allowed methods of remote access to the system;
b. Establishing usage restrictions and implementation guidance for each allowed remote access method;
c. Monitoring for unauthorized remote access to systems;
d. Authorizing remote access to systems prior to connection;
e. Enforcing requirements for remote connections to systems;
f. Using cryptography to protect the confidentiality and integrity of remote access sessions;
g. Automatically disconnecting remote access sessions after a period of inactivity; and
h. Immediately deactivating vendor and business partner remote access when it is no longer needed.

Remote Access includes:

Automated Monitoring / Control
Information systems must monitor and control remote access methods.

Protection of Confidentiality / Integrity Using Encryption
Information systems must implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Managed Access Control Points
Information systems must route all remote accesses through TTUHSC El Paso-managed network access control points.

Privileged Commands & Access
TTUHSC El Paso authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.

Telecommuting
TTUHSC El Paso authorizes remote users / teleworkers to connect to the internal network only if the following criteria for the remote system are met:

a. Software patch status is current; and
b. Anti-malware software is enabled and current.

Monitoring Vendor Usage
Asset custodians and data/process owners are responsible for managing vendor remote access accounts, as follows:

a. Vendor accounts may only be enabled only during the time period needed and must be disabled when not in use;
b. Vendor account usage must be monitored when in use.

Disconnect / Disable Remote Access
The Identity and Access Management (IAM) team must implement mechanisms to disconnect or disable remote access within fifteen (15) minutes of notice.

AC-18: Wireless Access

TTUHSC El Paso's IT department is responsible for:

a. Establishing usage restrictions and implementation guidance for wireless access;
b. Monitoring for unauthorized wireless access to the system;
c. Authorizing wireless access to systems prior to connection; and
d. Enforcing requirements for wireless connections to systems.
e. Ensuring SSID values are changed from the manufacturer default setting and;
f. Prohibiting and monitoring any unauthorized installation or use of Wireless Personal Area Networks on TTUHSC El Paso systems by individuals without the approval of the IT information resources manager.

AC-19: Access Control For Mobile Devices

For TTUHSC El Paso-owned mobile devices, the following is required:

a. Loss / Theft. Immediately notify TTUHSC El Paso management if a mobile device is lost or stolen and the user must alert management to the circumstance of the loss and the data contained on the mobile device.
b. Users must conduct themselves in accordance with TTUHSC El Paso's Acceptable Use parameters.

c. A password or PIN with a minimum of four (4) characters must be used to log onto the device.
d. Lockout. The mobile device must be set to delete all data or lock internally after ten (10) unsuccessful attempts to enter a password or PIN.
e. The data on the mobile device must be encrypted.
f. Message Storage Limits. Users may not store more than two hundred (200) messages or fourteen (14) days of messages on a mobile device.
g. Data Backups. If the user backs up the data from the mobile device to another device that is not encrypted (e.g., backing up a tablet using an unencrypted computer), then the backup data must be encrypted.
h. Software Protections. Applications that create, store, access, send or receive ePHI must meet TTUHSC El Paso security standards and custom developed applications used on mobile devices must undergo a security design review.
i. Anti-malware. Anti-malware software must be installed on mobile devices that are capable of running such software:
    i. Android: Android devices are required to have anti-malware software installed.
    ii. Windows: Windows devices are required to have anti-malware software installed.
    iii. Apple: The Apple iOS is not currently capable of running anti-malware software, since no such software exists, based on the design of the iOS.
j. Updates. Mobile device and installed applications must be kept updated with the latest vendor software releases:
    i. Operating Systems: The most recent operating system available for the mobile data device must be used.
    ii. Applications: Available security updates for any applications must be applied in a regular and timely manner unless instructed otherwise by TTUHSC El Paso IT staff.
k. Rooting. Users must not circumvent the security of mobile devices by removing limitations designed to protect the device (e.g., “jailbreaking”) and users must not tamper with the mobile device by using unauthorized software, hardware, or other methods.
l. Wireless. Users are required to utilize good judgment when connecting the mobile device to other devices and networks:
    i. Bluetooth: Passwords or PINs must be used to secure Bluetooth connections with devices and block unknown devices.
    ii. WiFi: Users may use only secure (e.g., WPA2) WiFi networks known to be trustworthy.
    iii. Cellular: TTUHSC El Paso is not responsible for overages or data plans for cellular usage.

Access Control for mobile devices includes:

Full Device / Container-Based Encryption
Information systems must employ full-device or container encryption to protect the confidentiality and integrity of information on TTUHSC El Paso-owned or managed mobile devices.

Central Management Of Mobile Devices
TTUHSC El Paso requires mobile devices to be:

a. Centrally managed; and
b. Have passwords enabled in accordance with TTUHSC El Paso’s existing password standards.

Remote Purging
TTUHSC El Paso requires mobile devices must be able to be remotely wiped when the mobile device is reported as lost or stolen.

Personally Owned Devices
TTUHSC El Paso assumes that all mobile devices are untrusted unless TTUHSC El Paso has properly secured the mobile device. When approved by TTUHSC El Paso management, users are allowed to use personally-owned mobile devices, only if the following conditions are met:

a. Conduct. Users must conduct themselves in accordance with TTUHSC El Paso’s Acceptable Use

parameters;

b. Passwords. A password or PIN with a minimum of four (4) characters must be used to log onto the device
c. Lockout. The mobile device must be set to delete all data or lock internally after ten (10) unsuccessful attempts to enter a password or PIN.
d. Encryption. The data on the mobile device must be encrypted.
e. Message Storage Limits. Users may not store more than two hundred (200) messages or fourteen (14) days of messages on a mobile device.
f. Data Backups. If the user backs up the data from the mobile device to another device that is not encrypted (e.g., backing up a tablet using an unencrypted computer) then the backup data must be encrypted.
g. Software Protections. Applications that create, store, access, send or receive ePHI must meet TTUHSC El Paso security standards and custom developed applications used on mobile devices must undergo a security design review.
h. Anti-malware. Anti-malware software must be installed on mobile devices that are capable of running such software:
    i. Android: Android devices are required to have anti-malware software installed.
    ii. Windows: Windows devices are required to have anti-malware software installed.
    iii. Apple: The Apple iOS is not currently capable of running anti-malware software, since no such software exists, based on the design of the iOS.
i. Updates. Mobile device and installed applications must be kept updated with the latest vendor software releases:
    i. Operating Systems: The most recent operating system available for the mobile data device must be used.
    ii. Applications: Available security updates for any applications must be applied in a regular and timely manner unless instructed otherwise by TTUHSC El Paso IT staff.
j. Rooting. Users must not circumvent the security of mobile devices by removing limitations designed to protect the device (e.g., “jailbreaking”) and users must not tamper with the mobile device by using unauthorized software, hardware, or other methods.
k. Wireless. Users are required to utilize good judgment when connecting the mobile device to other devices and networks:
    i. Bluetooth: Passwords or PINs must be used to secure Bluetooth connections with devices and block unknown devices.
    ii. WiFi: Users may use only secure (e.g., WPA2) WiFi networks known to be trustworthy.
    iii. Cellular: TTUHSC El Paso is not responsible for overages or data plans for cellular usage.
l. Storing. TTUHSC El Paso data outside of TTUHSC El Paso-approved, encrypted containers on the mobile device.

Tamper Protection & Detection
Users are required to:

a. Physically examine their mobile devices upon return from travel to locations of concern for signs of physical or logical tampering; and
b. Immediately report any possible tampering to TTUHSC El Paso.

AC-20: Use of External Information Systems

TTUHSC El Paso permits the use of external information systems to process, store and/or transmit TTUHSC El Paso data only when:

- A valid business reason exists for the external trust relationship;
- A formal risk assessment of the third-party has been conducted;
- Risks identified in the risk assessment have been adequately addressed, if applicable; and
- A formal contract exists, including Non-Disclosure Agreements (NDAs).

Use of External Information Systems includes:

Limits of Authorized Use
TTUHSC El Paso permits authorized individuals to use external information systems to access the TTUHSC El Paso systems or to process, store, or transmit TTUHSC El Paso-controlled information only when TTUHSC El Paso verifies the implementation of required security controls on the external system as specified in TTUHSC El Paso's information security policies and standards.

Portable Storage Devices
TTUHSC El Paso:

a. Restricts the use of TTUHSC El Paso-controlled portable storage devices by authorized individuals on external information systems; and
b. Prohibits personally-owned portable storage devices on external information systems.

AC-21: Information Sharing

TTUHSC El Paso:

- Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for information sharing circumstances where user discretion is required; and
- Employs a process to assist users in making information sharing/collaboration decisions.

While it is the user's responsibility to exercise sound judgment if information should be shared, asset custodians and data/process owners are required to:

a. Facilitate information sharing by enabling authorized users to use authorized technology (e.g., SharePoint, a blog, or a wiki page); and
b. Employ a process to assist users in making information sharing/collaboration decisions.

AC-22:Publicly Accessible Content

Asset custodians and data/process owners are required to:

a. Designate select individuals to be authorized to post information onto publicly accessible websites;
b. Train the authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c. Review the proposed content of publicly accessible information for nonpublic information prior to posting onto publicly accessible websites;
d. Review the content on the publicly accessible websites for nonpublic information; and
e. Remove nonpublic information from the publicly accessible websites, if discovered.

All other IT Policies can be found at https://ttuhscep.edu/it/policies/

TAC 202.74
56.50 Sanctions Policy (SN)
HIPAA 164.312(a)(a) | PDI DSS 8.1 & 8.4
HIPAA 164.312(d) | PCI DSS 8.1.3-8.1.5, 8.2.2, 8.5, 8.5.1, 8.6 &8.7 | MA201CMR17 17.04(1(a)) | NIST CSF PR.AC-1, PR.AC-4, DE.CM-1 & DE.CM-3
PCI.DSS 1.3.1
PCI.DSS 1.3.2
PCI.DSS 1.3.3
PCI.DSS 1.3.4
PCI.DSS 1.3.5

PCI.DSS 1.3.6
PCI.DSS 1.3.7
Saltzer, Jerome H. & Schroeder, Michael D. "The Protection of Information in Computer Systems. "Proceedings of the IEEE 63, 9 (September 1975): 1278-1308.
NIST CSF PR.AC-4
NIST CSF PR.IP-8