HSCEP OP: 56.50 – Configuration Management (CM)

Policy Statement:

TTUHSC El Paso shall maintain accurate inventories of its systems and enforce security configuration settings for information technology products employed in support of TTUHSC El Paso's business operations.

Reason for Policy:

The purpose of Configuration Management (CM) policy is to establish and maintain the integrity of systems.

What is covered in this Policy?

The overall policy addresses the institutional stance as it applies to TTUHSC El Paso in the areas of: configuration management, baseline configurations, change control, security impact analysis, access restriction for change, configuration settings, least functionality, system component inventory, configuration management plan, software usage restrictions, and user-installed software.

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 Sanctions Policy.

CM-01: Configuration Management Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates:

- A formal, documented configuration management 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 configuration management policy and associated configuration management controls.

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

a. A formal, documented configuration management policy; and
b. Processes to facilitate the implementation of the configuration management policy, procedures and associated controls.

CM-02: Baseline Configurations

TTUHSC El Paso develops, documents, and maintains under configuration control, a current baseline configuration for systems.

Asset custodians are required to review, update, test, and approve baseline configurations as an integral part of system installations and upgrades.

Baseline Configurations Include:

Reviews & Updates
Asset custodians are required to review and update baseline configurations for systems under their control:

a. At least annually;
b. When required to do so; or
c. As part of system component installations and upgrades.

Automation Support For Accuracy/Currency
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of information systems.

Retention Of Previous Configurations
Asset custodians are required to store and maintain at least three (3) previous versions of configurations to support rollback and troubleshooting operations.

Development & Test Environments
Asset custodians are required to maintain and manage baseline configurations for development and test environments separately from its production baseline configurations.

Configure Systems, Components Or Devices For High-Risk Areas
Where technically and/or economically feasible, TTUHSC El Paso must:

a. Issue information systems, system components, or devices with organization-defined configurations to individuals traveling to locations that TTUHSC El Paso deems to be of significant risk; and
b. Apply additional, TTUHSC El Paso-defined security safeguards to the devices when the individual(s) return.

Configuration File Synchronization
Where technically feasible, asset custodians responsible for network devices are required to verify running configuration files and start-up files are:

a. Synchronized with the correct build; and
b. The same secure configurations.

CM-03: Configuration Change Control

TTUHSC El Paso:

- Retains and reviews records of configuration-controlled changes to systems.
- Determines the type of changes to systems that are configuration controlled;
- Approves configuration-controlled changes to systems with explicit consideration for security impact analyses;
- Documents approved configuration-controlled changes to systems;
- Audits activities associated with configuration-controlled changes to systems; and
- Coordinates and provides oversight for configuration change control activities through an organization-defined configuration change control element (e.g., committee, board) that convenes on a routine basis.

Information Technology is required to test, validate, and document changes to systems before implementing the changes on the production network.

Configuration Change Controls Include:

Prohibition Of Changes

Asset custodians and data/process owners are prohibited from implementing a change without first obtaining pre-approval from Information Security and notifying all affected parties prior to the implementation of the change.

Test, Validate & Document Changes
Asset custodians and data/process owners are required to test configuration changes, wherever it is possible, to test a configuration, prior to deploying in the production environment.

Security Representative
TTUHSC El Paso's IT security personnel are required to represent IT topics as a representative of TTUHSC El Paso's Change Control Board.

CM-04: Security Impact Analysis

TTUHSC El Paso's analyzes changes to systems to determine potential security impacts prior to change implementation.

From a test environment, asset custodians are required to test proposed changes to assess the security functions of a system to verify that those functions are:

a. Implemented correctly;
b. Operating as intended; and
c. Producing the desired outcome with regard to meeting the security requirements for the system.

CM-05: Access Restriction For Change

TTUHSC El Paso defines documents, approves, and enforces access restrictions associated with changes to systems:

Information Technology is required to configure systems to prevent the installation of software and hardware components by non-administrators through limiting the actions that users are capable of performing.

Access Restriction Includes:

Automated Access Enforcement/Auditing
Where technically feasible information systems must enforce access restrictions and support auditing of the enforcement actions.

Signed Components
Where technically feasible information systems must prevent the installation of software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by TTUHSC El Paso.

Two-Person Rule
When dictated by a compensating control, asset custodians are required to develop and implement a two-person rule for implementing changes to sensitive system components and system-level information.

Limit Production/Operational Privileges (Incompatible Roles)
TTUHSC El Paso's management is required to:

1. Identify incompatible business roles;
2. Limit privileges to change information system components and system-related information within a production or operational environment;
3. Implement steps to remediate incompatible business roles; and
4. Perform reviews, based on TTUHSC El Paso's access permission review requirements.

Library Privileges
Data/process owners are required to limit privileges to change software archived within software

libraries.

CM-06: Configuration Settings

TTUHSC El Paso:

- Establishes and documents mandatory configuration settings for information technology products using industry-recognized leading practices consistent with operational requirements;
- Implements the configuration settings;
- Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within systems based on explicit operational requirements; and
- Monitors and controls change to the configuration settings in accordance with organizational policies and procedures.

TTUHSC El Paso is required to establish configuration standards for all technology platforms, including but not limited to:

a. Firewalls;
b. Routers;
c. Switches, capable of being managed;
d. Wireless Access Points (WAPs)'
e. Servers;
f. Workstations; and
g. Mobile Devices, capable of being managed

Configuration Settings Includes:

Automated Central Management/Application/Verification
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall employ automated mechanisms to centrally manage, apply, and verify configuration settings for information system components.

Respond To Unauthorized Changes
Upon identifying an unauthorized change to an approved configuration setting, users are required to report the unauthorized change to TTUHSC El Paso's IT security personnel.

CM-07: Least Functionality

TTUHSC El Paso configures systems to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services.

TTUHSC El Paso utilizes the "principle of least privilege,"11 which states that only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary. Asset custodians are required to the following:

a. Identifying and removing insecure services, protocols, and ports;
b. Enabling only necessary and secure services, protocols, and daemons, as required for the function of the system;
c. Implementing security features for any required services, protocols or daemons that are considered to be insecure (e.g., NetBios, Telnet, FTP, etc.);
d. Verifying services, protocols, and ports are documented and properly implemented by examining firewall and router configuration settings; and
e. Removing all unnecessary functionality, such as:
    1. Scripts;
    2. Drivers;
    3. Features;
    4. Subsystems;
    5. File systems; and
    6. Unnecessary web servers.

Least Functionality Includes:

Periodic Review
Asset custodians are required to:

a. Periodically review their systems to identify non-secure functions, ports, protocols, and services; and
b. Disable unnecessary and non-secure functions, ports, protocols, and services.

Prevent Program Execution
Asset custodians are required to configuring systems to employ automated mechanisms to prevent program execution of unauthorized software programs.

Unauthorized Or Authorized Software/Blacklisting Or Whitelisting
Where technically feasible and a business justification exists, TTUHSC El Paso may implement application blacklisting or whitelisting.

CM-08: Information System Component Inventory

TTUHSC El Paso develops, documents, and maintains an inventory of system components that:

- Accurately reflects the current system;
- Is at the level of granularity deemed necessary for tracking and reporting;
- Includes organization-defined information deemed necessary to achieve effective property accountability; and
- Is available for review and audit by designated organizational officials.

TTUHSC El Paso is required to create, maintain, and update an inventory of its assets.

Information System Component Inventory Includes:

Updates During Installations/Removals
Where technically feasible, asset custodians must update the inventory of information system components as an integral part of component installations, removals, and information system updates.

Automated Unauthorized Component Detection
If applicable, TTUHSC El Paso's management of Network Access Control (NAC) technologies:

- Employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
- Takes action when unauthorized components are detected.

No Duplicate Accounting Of Components
Where technically feasible asset custodians must verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

Approved Deviations
Asset custodians are required to request and document approved deviations to deployed configurations in a system under their control.

Network Diagrams
Asset custodians and data/process owners are required to:

a. Verify that a current network diagram exists for their environment(s);
b. Maintain a current diagram that shows all cardholder data flows across systems and networks; and
c. Documents all connections, including any wireless networks and hosted services.

Network Access Control (Nac)
If applicable, TTUHSC El Paso's management of Network Access Control (NAC) technologies:

a. Require the identification, organization, and categorization of key resources, devices and users,
b. Must be mapped to TTUHSC El Paso's least functionality controls; and
c. Requires updating as resources, devices, and users change and evolve.

CM-09: Configuration Management Plan

TTUHSC El Paso develops, documents, and implements a configuration management plan for systems that:14

- Addresses roles, responsibilities, and configuration management processes and procedures;
- Defines the configuration items for systems and when in the system development life cycle the configuration items are placed under configuration management; and
- Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

Where technically feasible, asset custodians and data/process owners are required to configure systems to include a description of groups, roles, and responsibilities for the logical management of those devices.

CM-10: Software Usage Restrictions

TTUHSC El Paso:

- Uses software and associated documentation in accordance with contract agreements and copyright laws;
- Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and
- Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Users are required to implement and utilize software in accordance with license agreements and copyright laws.

Software Usage Restrictions Include:

Open Source Software
Only when a strong business case exists and a risk assessment supports it is open source software approved for use.

CM-11: User-Installed Software

TTUHSC El Paso enforces explicit rules governing the installation of software by users.

Software installation is permitted only by authorized system administrators.

User-Installed Software Includes:

Unauthorized Installation Alerts
Where technically feasible, alerting is required to be configured to notify appropriate asset custodians or IT security personnel when the unauthorized installation of software is detected.

Prohibiting Installation Without Privileged Status
Software installation is permitted only by authorized system administrators.

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

1. 56.50 Sanctions Policy (SN)
2. PCI DSS 1.1.1 | NIST CSF PR.DS-7, PR.IP-1 & DE.AS-1 | DFARS 252.204-7008

3. DISA STIGs official site: http://iase.disa.mil/stigs/index.html

4. PCI SS 6.4.1

5. PCI DSS 1.2.2

6. NIT CSF PR.IP-1, PR.IP-3, DE.CM-1 & DE.CM-7

7. PCI DSS 6.4, 6.4.5, 6.4.5.1-6.4.5.4 | NIST CSF PR.IP-1 & PR.IP-3

8. NIST CSF PR.IP-1

9. PCI DSS 1.1 & 1/1/1 | NIST CSF PR.IP-1

10. PCI DSS 1.1.5, 1.2.1, 2.2.2, 2.2.4 & 2.2.5 | MA201CMR17 17.03(2)(a) | NIST CSF PR.IP-1

11. Saltzer, Jerome H. & Schroeder, Michael D. "The Protection of Information in Computer Systems." Proceedings of the IEEE 63, 9 (September 1975): 1278-1308.

12. HIPAA 164.310(d)(b)(iii) | PCI DSS 1.1.2 | NIST CSF ID.AM-1, ID.AM-2, PR.DS-3, PR.PT-3 & DE.CM-7

13. PCI DSS 1.1.1 & 1.1.3

14. PCI DSS 1/1/5 | NIST CSF PR.IP-1

15. NIST CSF DE.CM-3

16. NIST CSF DE.CM-3

17. TAC §202.74, TAC §202.75

Revised May 2018