HSCEP OP: System & Service Acquisition (SA)

Policy Statement:

TTUHSC El Paso shall allocate sufficient resources to adequately protect organizational systems by employing a System Development Life Cycle (SDLC) process that incorporate IT security considerations.

Reason for Policy:

The purpose of the System & Services Acquisition (SA) policy is to ensure that systems employ a System Development Life Cycle (SCLD), where the security of systems and services are assessed throughout the operational life of the systems to reduce risks to TTUHSC El Paso.

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: maintenance, controlled maintenance, tools, non-local maintenance, maintenance personnel, and timely maintenance.

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, Sanctions Policy.

SA-01: System & Services Acquisition 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.

SA-02: Allocation of Resources

TTUHSC El Paso:

- Includes a determination of information security requirements for systems in business process planning;
- determines, documents, and allocates the resources required to protect systems as part of its capital planning and investment control process; and
- Establishes a discrete line item for information security in organizational programming and budgeting documentation.

TTUHSC El Paso is required to:

- Include information security requirements in business process planning; and
- Allocate resources required to protect its systems and data, as part of its capital planning process.

SA-03: System Development Life Cycle (SDLC)

TTUHSC El Paso.

- Manages systems using a System Development Life Cycle (SDLC) methodology that includes information security considerations; and
- Defines and documents system security roles and responsibilities throughout the SDLC.

  For all significant development and/or acquisitions, asset custodians and data/process owners are required to:

- Manage systems using a System Development Life Cycle (SDLC) that includes information security considerations; and
- Define and document information security roles and responsibilities throughout the SDLC

SA-04: Acquisition Process

TTUHSC El Paso's includes the following requirements and/or specifications, explicitly or by reference, in system acquisitions based on an assessment of risk:

- Security functional requirements/specifications;
- Security-related documentation requirements; and
- Developmental and evaluation-related security requirements.

Asset custodians and data/process owners are required to take security requirements into account when purchasing systems or outsourcing solutions to comply with CIS Level 1 standards and benchmarks.

Acquisition Process includes:

Functional Properties Of Security Controls
Vendors are required to provide documentation describing the functional properties of the security controls employed within systems, system components, or system services in sufficient detail to permit analysis and testing of the controls.

Design & Implementation of Security Controls
Vendors are required to provide documentation describing the design and implementation the security controls employed within systems, system components, or system services in sufficient detail to permit analysis and testing of the controls.

Development Methods
Software vendors are required to demonstrate that their software development processes employ:

a. Industry-recognized leading practices for secure programming;
b. Secure engineering methods;
c. Quality control processes; and
d. Testing processes to minimize flawed or malformed software.

Commercial Off-The-Shelf (COTS) Security Solutions
TTUHSC El Paso is required to use only Commercial Off-the-Shelf (COTS) products for information security requirements.

Continuous Monitoring Plan
Where technically feasible and justified by a valid business case, third-party developers of information system, system component, or information system service are required to produce a plan for the continuous monitoring of security control effectiveness.

Functions/Ports/Protocols/Services In Use
TTUHSC El Paso requires that developer of information systems, system components, or information system services to identify early in the system development life cycle, the functions, ports, protocols, and services intended that will be enabled for use in a production environment.

Use of Approved PIV Products
Where technically feasible, TTUHSC El Paso employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

SA-05: Access Restriction for change.

TTUHSC El Paso:

- Obtains, protects as required, and makes available to authorized personnel, administrator documentation for systems that describes:
    - Secure configuration, installation, and operation of the system;
    - Effective use and maintenance of security features/functions; and
    - Known vulnerabilities regarding configuration and use of administrative (e.g.,) functions; and
- Obtains, protects as required, and makes available to authorized personnel, user documentation for systems that describes:
    - User-accessible security features/functions and how to effectively use those security features/functions;
    - Methods for user interaction with systems, which enables individuals to use the system in a more secure manner; and
    - User responsibilities in maintaining the security of the information and system; and
- Documented attempts to obtain system documentation when such documentation is either unavailable or nonexistent.

Asset custodians and data/process owners are required to:

a. obtain administrator documentation for systems that describes:
    i. Secure configuration, installation, and operation of the system;
    ii. Effective use and maintenance of security features/functions; and
    iii. Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions;
b. Obtain user documentation for systems that describes:
    1. User-accessible security features/functions and how to effectively use those security features/functions;
    2. Methods for user interaction with the system, which enables individuals to use the system in

a more secure manner; and
3. User responsibilities in maintaining the security of the information and system.

Information System Documentation includes:

Functional Properties Of Security Controls
Developers are required to provide asset custodians documentation describing the functional properties of the security controls employed within systems, system components, or system services in sufficient detail to permit analysis and testing of the controls.

External System Interfaces
Developers are required to provide documentation describing external system interfaces (e.g., data connections) in sufficient detail to permit monitoring and testing.

High-Level Design
Developers are required to provide asset custodians documentation in sufficient detail to permit high-level analysis and an architectural review.

Low-Level Design
Developers are required to provide asset custodians documentation in sufficient detail to permit detailed analysis and control testing.

SA-06: Software Usage Restrictions
Incorporated into CM-10 & SI-07

SA-07: User-Installed Software
Incorporated into CM-11 & SI-07

SA-08: Security Engineering Principles

TTUHSC El Paso applies industry-recognized leading practices engineering principles in the specification, design, development, implementation, and modification of systems.5

Asset custodians are required to implement configuration standards for all system components that address known security vulnerabilities and are consistent with industry-accepted system hardening standards which are CIS Level 1 baseline standards and configuration.

SA-09: External Information System Services
If TTUHSC El Paso outsources IT-related activities, the organization:6

- Conducts an organizational assessment of risk prior to the acquisition or outsourcing of services;
- Maintains and implements policies and procedures to manage service providers (e.g., Software-as-a-Service (SaaS)., Web hosting companies, collection providers, or email providers), through observation, review of policies and procedures, and review of supporting documentation. Including:
  - Maintaining a list of service providers.
  - Maintaining a written agreement that includes an acknowledgment that the service providers are responsible for the security of data the service providers possess.
  - Ensuring there is an established process for engaging service providers including proper due diligence prior to engagement.
- Maintains a program to monitor service providers' control compliance status at least annually.
- Requires that providers of external system services comply with organizational information security requirements and employ appropriate security controls in accordance with local, state and Federal laws, as well as all applicable regulatory requirements;
- Defines and documents oversight and user roles and responsibilities with regard to external

system services; and
- Conducts an organizational assessment of risk prior to the acquisition or outsourcing of services.

Asset custodians and data/process owners are required to:

a. Maintain a comprehensive list of service providers, including all applicable Service Level Agreements (SLAs);
b. Require that providers of external systems comply with TTUHSC El Paso information security requirements and employ appropriate security controls in accordance with local, state and Federal laws, as well as all applicable regulatory requirements;
c. Define oversight responsibilities with regard to external system services;
d. Perform a review of the service provided for acceptable service levels;
e. Conduct a risk assessment outsourcing of services; and
f. Monitor security control compliance by external service providers.

External Information System Services Include:

Risk Assessment & Organizational Approvals

Asset custodians and data/process owners are required to:

a. Conduct a risk assessment outsourcing of services;
b. Assume responsibility for any TTUHSC El Paso-owned or managed device used to connect TTUHSC El Paso's network to an external system service.
c. Maintain a comprehensive list of service providers, including all applicable Service Level Agreements (SLAs);
d. Require that providers of external systems comply with TTUHSC El Paso requirements and employ appropriate security controls in accordance with all applicable laws and regulatory requirements;
e. Define oversight responsibilities with regard to external system services;
f. Review affected client contracts/projects to determine if notification to the client is necessary if a service provider is terminated;
g. Monitor security control compliance by external service providers; and
h. Maintain information about which PCI DSS requirements are managed by each service provider and which are managed by TTUHSC El Paso, where applicable.

Identification Of Functions, Ports, Protocols & Services

Data/process owners, in conjunction with asset custodians, are required to develop documentation that describes the functions, ports, protocols, and services necessary for systems or applications to interact with TTUHSC El Paso's network.

Business Partner Contracts

TTUHSC El Paso is required to maintain written and executed agreements with business partners to ensure:8

a. Appropriate management, operational and technical control safeguards are in place to ensure the confidentiality, integrity, and availability of TTUHSC El Paso's sensitive data the business associate creates, receives, maintains, or transmits; and
b. Service providers acknowledge in writing that they are responsible for the security of TTUHSC El Paso data (e.g., cardholder data) that the service provider possesses or otherwise stores, processes, or transmits on behalf of TTUHSC El Paso, or to the extent that they could impact the security of TTUHSC El Paso data environment.

Consistent Interests Of Consumers And Providers

Data/process owners are required to ensure appropriate security safeguards are implemented to ensure that the interests of external service providers are consistent with and reflect TTUHSC El Paso's interests.

Processing, Storage And Service Location

Data/process owners are required to ensure the location(s) of information processing/storage is compliant with TTUHSC El Paso's business requirements.

Group Health Plans
Asset custodians and data/process owners are required to ensure electronic Protected Health Information (ePHI) is reasonably and appropriately safeguarded when creating, receiving, maintaining or transmitting data on behalf of an employee, contractor or group health plan.

SA-10: Developer Configuration Management

TTUHSC El Paso requires that system developers and integrators:

- Perform configuration management during system design, development, implementation, and operation;
- Manage and control changes to systems;
- mplement only organization-approved changes;
- Document approved changes to systems; and
- Track security flaws and flaw resolution.

TTUHSC El Paso requires that system developers and integrators:

- Perform configuration management during system design, development, implementation, and operation that complies with CIS Level 1 standards and configuration benchmarks;
- Manage and control changes to systems;
- Implement only company-approved changes;
- Document approved changes to systems; and
- Track security flaws and flaw resolution.

Developer Configuration Management Includes:

Software/Firmware Integrity Verification

Where technically and a business justification exists, asset owners will ensure File Integrity Monitoring (FIM) mechanisms exist and are configured to alert security personnel when unauthorized changes are made.

SA-11: Developer Security Testing

TTUHSC El Paso requires that system developers/integrators, in consultation with associated security personnel:

- Create and implement a security test and evaluation plan;
- Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and
- Document the results of the security testing/evaluation and flaw remediation processes.

Developers and system integrators are required to:

a. Follow change control processes and procedures for all changes to system components that affect TTUHSC El Paso's production network;
b. Remove test data and accounts before production systems become active/ goes into production; and
c. Ensure security functionality testing is conducted, prior to implementation.

Developer Security Testing Includes:

Static Code Analysis

Developers and system integrators are required to perform a static code analysis of custom code prior to release to production or customers, in order to identify any potential coding vulnerability.

Threat Analysis & Flaw Remediation
Asset custodians and data/process owners are required to:

a. Address new threats and vulnerabilities on an ongoing basis and ensures these applications are protected against known attacks by either of the following methods:

   i. Reviewing applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; or
   ii. Installing an application firewall.

b. Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows:

   i. At least annually;
   ii. After any changes;
   iii. By an organization that specializes in application security;
   iv. That all vulnerabilities are corrected; and
   v. That the application is re-evaluated after the corrections

Dynamic Code Analysis

Developers and system integrators are required to employ dynamic code analysis tools to review custom code prior to release to production or customers, in order to identify any potential coding vulnerability.

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

56.50 Disciplinary Process (DI)
NIST CSF PR.IP-2
NIST CSF PR.IP-2 & DE.CM-6
4. NIST CSF ID.RA-1
5. PCI DSS 2.2 | NIST CSF PR.IP-2
6. MA201CMR17 17.03(2)(f)(a) | OR646A.622(2)(d)(A)(v) | NIST CSF ID.AM-4, PR.AT-3 & DE.CM-6
7. HIPAA 164.308(a)(2)(a). 164.308(a)(4)(a) & 164.314(a) | GLBA Safeguards Rule | PCI DSS 2.4,12.8-12.8.4 | MA201CMR17 17.03(2)(f)(b) | OR646A.622(2)(d)(A)(v)
8. HIPAA 164.308(b)(a), 164.314(a)(1)(i)-(ii), 164.314(a)(1)(ii)(A)-(B), 164.314 (a)(2)(i)(A)-(D), 164.314(a)(2)(i)(A)-(D), 164.314(a)(2)(ii)(a)-(b) | PCI DSS 2.6 & 12.9
9. HIPAA 164.314(b)(a)-(b) | PCI DSS 12.9
10. MA201CMR17 17.03(2)(d)(B)(i) | NIST CSF PR.IP-1, PR.IP-2 & PR.IP-3
11. PCI DSS 6.4 & 6.4.4 | MA201CMR17 17.03(2)(d)(B)(i) | NIST CSF ID.RA-1 & PR.IP-2
12. PCI DSS 6.3, 6.3.1 & 6.3.2
13. PCI DSS 6.6
14. TAC§202.76

Revised May 2018