HEART OF TEXAS WORKFORCE DEVELOPMENT BOARD, INC.

POLICY

ID NO.:	HWD CS 010-23	**DATE ISSUED:**	3/1/2023
PROGRAM:	Cybersecurity	**KEYWORD:**	System and Services Acquisition Policy

SUBJECT: System and Services Acquisition Policy

PURPOSE: To provide staff with information and guidance on the requirements, expectations, and oversight of System and Services Acquisitions within the Heart of Texas Workforce Solutions environment.

REFERENCES: ?????

POLICY: SYSTEM AND SERVICES ACQUISITION POLICY

GENERAL POLICY

The Heart of Texas Workforce Workforce Development Board (HOTWDB) Information Technology Security Steering Committee(ITSSC) will develop, document, and disseminate a System and Services Acquisition policy and procedures that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

The HOTWD ITSSC will review and update the current System and Services Acquisition policy and procedures at least annually.

Allocation of Resources
The HOTWDB ITSSC will determine high-level security and privacy requirements for the system or system service in mission/business process planning.

The HOTWDB ITSSC will determine, document, and allocate the resources required to protect the system or system service as part of its capital planning and investment control process.

The HOTWDB ITSSC will establish a discrete line item for security and privacy in organizational programming and budgeting documentation.

System Development Lifecycle
The Heart of Texas Workforce Solutions Technology Department will acquire, develop, and manage the information system using the *defined system development life cycle* that incorporates information security and privacy considerations.

The HOTWDB ITSSC will define and document information security roles and responsibilities throughout the system development life cycle.

The HOTWDB ITSSC will identify individuals having security and privacy roles and responsibilities.

The HOTWDB ITSSC will integrate the organizational information security and privacy risk management process into system development life cycle activities.

Acquisition Process
The HOTWDB ITSSC will include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

1. Security and privacy functional requirements.
2. Strength of mechanism requirements.
3. Security and privacy assurance requirements.
4. Controls needed to satisfy the security and privacy requirements.
5. Security and privacy documentation requirements.
6. Requirements for protecting security-related documentation.
7. Description of the system development environment and environment in which the system is intended to operate.

8. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management.
9. Acceptance criteria.

Information System Documentation
The Heart of Texas Workforce Solutions Technology Department will obtain or develop administrator documentation for the system, system component, or system service that describes:

1. Secure configuration, installation, and operation of the system, component, or service;
2. Effective use and maintenance of security and privacy functions/mechanisms; and
3. Known vulnerabilities regarding configuration and use of administrative or privileged functions

The Heart of Texas Workforce Solutions Technology Department will obtain user documentation for the information system, system component, or information system service that describes:

1. User-accessible security and privacy functions/mechanisms and how to effectively use those security functions/mechanisms
2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
3. User responsibilities in maintaining the security of the system, component, or service

The Heart of Texas Workforce Solutions Technology Department will document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes appropriate actions in response.

The HOTWDB ITSSC will distribute documentation to those with a need to know.

Security Engineering Principles
The Heart of Texas Workforce Solutions Technology Department will apply the following system security and privacy engineering data governance principles in the specification, design, development, implementation, and modification of the system and system components.

- Document data systems
- Validate system protections/transmissions
- Validate stakeholder awareness and documentation
- Support discussion with data system owners and third-party vendors
- Perform ongoing review of Federal State and local requirements
- Validate policies and procedures comply with federal, state and local requirements

External Information System Services
The Heart of Texas Workforce Solutions Technology Department will require that providers of external system services comply with organizational information security and privacy requirements and employ *security controls* in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

The HOTWDB ITSSC will define and document organizational oversight and user roles and responsibilities regarding external system services.

The Heart of Texas Workforce Solutions Technology Department will employ *processes, methods, and techniques* to monitor security control compliance by external service providers on an ongoing basis.

Developer Configuration Management

The Heart of Texas Workforce Solutions Technology Department requires the developer of the system, system component, or information system service to:

1. Perform configuration management during system, component, or service *design, development, implementation, and operation*.
2. Document, manage, and control the integrity of changes to items under configuration management.
3. Implement only organization-approved changes to the system, component, or service.
4. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes.
5. Track security flaws and flaw resolution within the system, component, or service and report findings to authorized parties.

Developer Security Testing and Evaluation

The Heart of Texas Workforce Solutions Technology Department requires the developer of the system, system component, or system service, at post-design stages of the system development lifecycle to:

a. Develop and implement a security and privacy control assessment plan.

b. Perform approved testing/evaluation *(unit; integration; system; regression)*

c. Produce evidence of the execution of the assessment plan and the results of the testing/evaluation.

d. Implement a verifiable flaw remediation process.

e. Correct flaws identified during security testing/evaluation.

Unsupported System Components

The Heart of Texas Workforce Solutions Technology Department will replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.

The HOTWDB ITSSC will provide justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

DOCUMENT CONTROL

Document Name	System and Services Acquisition
Document Control Number	TCF 11, 15, and 16

Document Identification	Version 1.0
Owner/Approver Identification	Technology Department
Author	Matilda Alonzo
Document Reviewer(s)	HOTWDB IT Security Steering Committee
Review Plan	This document should be reviewed by all parties on a regular basis. Next Review is: 3/1/2024
Latest Version	
Distribution	The Primary version of this document is stored in S:\Policies\Cybersecurity PRINTED COPIES OF THIS DOCUMENT ARE FOR REFERENCE ONLY!