BLINN COLLEGE ADMINISTRATIVE REGULATIONS MANUAL

SUBJECT: *Information Systems and Services*
EFFECTIVE DATE: June 1, 2020; amended September 19, 2023
BOARD POLICY REFERENCE: CS

PURPOSE

Develop policies and procedures for system and services.

PROCESS

System and Services Policy and Procedures (SA-01)

The College District:

A. Develops, documents, and disseminates to budget managers:
   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and

B. Reviews and updates the current:
   1. System and services acquisition policy biennially; and
   2. System and services acquisition procedures annually.

SYSTEM AND SERVICES POLICY

Allocation of Resources (SA-02)

The College District:

A. Determines information security requirements for the information system or information system service in mission/business process planning;
B. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
C. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

System Development Life Cycle (SA-03)

The College District:

A. Acquire, develop, and manage the system using a recognized risk mitigation framework that incorporates information security and privacy considerations;
B. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;
C. Identify individuals having information security and privacy roles and responsibilities; and
D. Integrate the organizational information security and privacy risk management process into system development life cycle activities.

Acquisition Process (SA-04)

The College District includes 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:

A. Security functional requirements;
B. Security strength requirements;
C. Security and privacy assurance requirements;
D. Controls needed to satisfy the security and privacy requirements.
E. Security and privacy documentation requirements;
F. Requirements for protecting security and privacy documentation;
G. Description of the system development environment and environment in which the system is intended to operate;
H. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and
I. Acceptance criteria.

Before acquisition, information technology or processing systems receiving, containing or processing personally identifiable information, protected health information or institutional data whether operating on premise or in the cloud must be reviewed and approved by the CISO and legal department.

Information System Documentation (SA-05)

The College District:

A. Obtains administrator documentation for the information system, system component, or information system service that describes:
    1. Secure configuration, installation, and operation of the system, component, or service;
    2. Effective use and maintenance of security functions/mechanisms; and
    3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
B. Obtains user documentation for the information system, system component, or information system service that describes:
    1. User-accessible security 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
    3. User responsibilities in maintaining the security of the system, component, or service;
C. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and is retained by the information system owner in response;
D. Protects documentation as required, in accordance with the risk management strategy; and
E. Distributes documentation to information system custodians and applicable documentation to users.

Security and Privacy Engineering Principles (SA-08)

Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: NIST 800-37 Rev. 2.

External System Services (SA-09)

The College District:

A. Requires providers of external information system services comply with college information security requirements and comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
B. Information system owners are responsible for oversight, defining user roles and responsibilities; and
C. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: TX-RAMP.

Developer Configuration Management (SA-10)

The College District requires the developer of the information system, system component, or information system service to:

A. Perform configuration management during system, component, or service design, development, implementation and operation;
B. Document, manage, and control the integrity of changes;
C. Implement only college-approved changes to the system, component, or service through the change control process;
D. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
E. Track security flaws and flaw resolution within the system, component, or service and report findings to information system owner and CISO.

Developer Testing and Evaluation (SA-11)

The College District requires the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

A. Develop and implement a plan for ongoing security and privacy assessments;
B. Perform system testing/evaluation;
C. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;
D. Implement a verifiable flaw remediation process; and
E. Correct flaws identified during testing and evaluation.

Unsupported System Components (SA-22)

A. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or
B. Provide the support from external providers.