BLINN COLLEGE ADMINISTRATIVE REGULATIONS MANUAL

SUBJECT: *Information Systems Security Planning*
EFFECTIVE DATE: March 1, 2020; amended September 19, 2023
BOARD POLICY REFERENCE: CS

PURPOSE

Develop policies and procedures for security planning.

PROCESS

Security Planning Policy and Procedures (PL-01)

The College District

A. Develops, documents, and disseminates to information system owners:
    1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    3. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
B. Reviews and updates the current:
    1. Security planning policy biennially; and
    2. Security planning procedures annually.

Security Planning Policy

The CISO must direct and coordinate the creation of a security plan protecting the information system assets of the College District. The plan must address the information systems' identification and classification, owners, automated protection tools, network security, minimum levels of system security settings, security audit process and frequency. In addition:

System Security and Privacy Plans (PL-02)

The College District

A. Develops a security plan for the information system that:
    1. Is consistent with the organization's enterprise architecture;
    2. Explicitly defines the authorization boundary for the system;
    3. Describes the operational context of the information system in terms of missions and business processes;
    4. Provides the security categorization of the information system including supporting rationale;
    5. Describes the operational environment for the information system and relationships with or connections to other information systems;
    6. Provides an overview of the security requirements for the system;
    7. Identifies any relevant overlays, if applicable;

8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
10. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
11. Include risk determinations for security and privacy architecture and design decisions;
12. Include security- and privacy-related activities affecting the system that require planning and coordination with information system owner and CISO; and
13. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

B. Distributes copies of the security plan and communicates subsequent changes to the plan to information system owners
C. Reviews the security plan for the information system annually;
D. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
E. Protects the security plan from unauthorized disclosure and modification.

Rules of Behavior (PL-04)

The College District

A. Establishes and makes readily available to individuals requiring access to the information system, the rules describing their responsibilities and expected behavior with regard to information and information system usage;
B. Include in the rules of behavior, restrictions on:
    1. Use of social media, social networking sites, and external sites/applications;
    2. Posting organizational information on public websites; and
    3. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.
C. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
D. Reviews and updates the rules of behavior biennially; and
E. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

Baseline Selection (PL-10)

The default baseline for an information system shall be the controls contained in the Security Controls Catalog (Information Systems Administrative Regulations).

The College District head may employ standards for the cost-effective information security of information, information resources, and applications within or under the supervision of the College District that are more stringent than the standards the DIR prescribes under this section if the more stringent standards:

A. contain at least the applicable standards issued by the department; and/or
B. are consistent with applicable federal law, policies, and guidelines issued under state rule, industry standards, best practices, or deemed necessary to adequately protect the information held by the College District.

Baseline Tailoring (PL-11)

The College District head may employ standards for the cost-effective information security of information, information resources, and applications within or under the supervision of the College District that are more stringent than the standards the DIR prescribes under this section if the more stringent standards:

A. contain at least the applicable standards issued by the department; and/or
B. are consistent with applicable federal law, policies, and guidelines issued under state rule, industry standards, best practices, or deemed necessary to adequately protect the information held by the College District.