BLINN COLLEGE ADMINISTRATIVE REGULATIONS MANUAL

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

PURPOSE

Develop policies and procedures for security program.

PROCESS

Information Security Program Plan (PM-01)

The College District

A. Develops and disseminates an organization-wide information security program plan that:
    1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
    2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
    3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
    4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
B. Reviews the organization-wide information security program annually;
C. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
D. Protects the information security program plan from unauthorized disclosure and modification.

Senior Information Security (PM-02)

The College District appoints a senior information security officer (CISO) with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

The Information Security Officer is charged with the responsibilities enumerated at Texas Government Code §2054.136 and 1 Texas Administrative Code §202.21.

Information Security Resources (PM-03)

The College District

A. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;
B. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and
C. Ensures that information security resources are available for expenditure as planned.

Plan of Action and Milestones (PM-04)

The College District

A. Implements a process ensuring plans of action and milestones for the security program and associated organizational information systems:
    1. Are developed and maintained;
    2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
    3. Are reported in accordance with OMB FISMA reporting requirements.
B. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Information Security Inventory (PM-05)

The College District develops and maintains an inventory of its information systems. The physical inventory must be maintained in the technology help desk system.

Information Security Measures of Performance (PM-06)

The College District develops, monitors, and reports on the results of information security measures of performance.

Monthly security reports must be submitted to the Department of Information Resources per their requirements.

Annual security program vulnerability assessment is presented and acknowledge by the College District CEO.

Enterprise Architecture (PM-07)

The College District develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

The director of Administrative Computing and dean of Academic Technology must develop an enterprise architecture in consideration of information security and risks to College District data and operations.

Risk Management Strategy (PM-09)

A. Develops a comprehensive strategy to manage:
    a. Security risk to organizational operations and assets, individuals, other organizations, the State of Texas, and the Nation associated with the operation and use of organizational systems; and
    b. Privacy risk to individuals resulting from the authorized processing of personally identifiable information;
B. Implement the risk management strategy consistently across the organization; and
C. Review and update the risk management strategy annually or as required, to address organizational changes.
D. **Authorization Process (PM-10)**
E. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;
F. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
G. Integrate the authorization processes into an organization-wide risk management program.

Testing, Training and Monitoring (PM-14)

A. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:
    a. Are developed and maintained; and
    b. Continue to be executed; and
B. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

Security and Privacy Groups and Associations (PM-15)

Establish and institutionalize contact with selected groups and associations within the security and privacy communities:

A. To facilitate ongoing security and privacy education and training for organizational personnel;
B. To maintain currency with recommended security and privacy practices, techniques, and technologies; and
C. To share current security and privacy information, including threats, vulnerabilities, and incidents.

Threat Awareness Program (PM-16)

The College District implements a threat awareness program that includes a cross-organization information-sharing capability.

The CISO must develop a threat awareness program sharing cybersecurity information amongst information system owners, yearly cybersecurity awareness training for employees and training as part of new employee orientation.