BLINN COLLEGE ADMINISTRATIVE REGULATIONS MANUAL

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

PURPOSE

Develop policies and procedures for information system incident response.

PROCESS

Incident Response Policy and Planning (IR-01)

The College District

A. Develops, documents, and disseminates to information resource owners or custodians and third parties:
   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

B. Reviews and updates the current:
   1. Incident response policy biennially; and
   2. Incident response procedures annually.

Incident Response Training (IR-02)

The College District provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within 60 days of assuming an incident response role or responsibility; b. When required by information system changes; and c. annually thereafter.

Incident Response Testing (IR-03)

Test the effectiveness of the incident response capability for the system annually using the following tests: tabletop exercises.

Incident Handling (IR-04)

The College District

A. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
B. Coordinates incident handling activities with contingency planning activities; and
C. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Incident Monitoring (IR-05)

The College District tracks and documents information system security incidents using a combination of logging and alerts from information security systems. Correlation of information systems event logging. Both automated and human based detection is utilized. Incident remediation is tracked using the technology help desk system with appropriate subject catalog classification.

Incident Reporting (IR-06)

The College District

A. Requires personnel to report suspected security incidents to the Academic Technology Help Desk immediately; and
B. Reports security incident information to the CISO.

The CISO must follow information security incident reporting requirements designated by the Department of Information Resources.

Reporting of security incidents and the investigation and restoration of operations following a security incident assessed to involve suspected criminal activity shall comply with 1 Texas Administrative Code § 202.23(b).

Incident Response Assistance (IR-07)

The College District provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

The CISO and the IT Security team form the core resource to assist users.

Incident Response Plan (IR-08)

The College District

A. Develops an incident response plan that:
    1. Provides the organization with a roadmap for implementing its incident response capability;
    2. Describes the structure and organization of the incident response capability;
    3. Provides a high-level approach for how the incident response capability fits into the overall organization;
    4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
    5. Defines reportable incidents;
    6. Provides metrics for measuring the incident response capability within the organization;
    7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
    8. Is reviewed and approved by CISO;
B. Distributes copies of the incident response plan to information resource owners;
C. Reviews the incident response plan annually;
D. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
E. Communicates incident response plan changes to information system owners and
F. Protects the incident response plan from unauthorized disclosure and modification.

Information Spillage Response (IR-09)

Respond to information spills by:

A. Assigning an incident responder with responsibility for responding to information spills;
B. Identifying the specific information involved in the system contamination;
C. Alerting CISO and executive leadership of the information spill using a method of communication not associated with the spill;
D. Isolating the contaminated system or system component;
E. Eradicating the information from the contaminated system or component;
F. Identifying other systems or system components that may have been subsequently contaminated; and
G. Performing additional actions in accordance with the incident response plan.