BLINN COLLEGE ADMINISTRATIVE REGULATIONS MANUAL

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

PURPOSE

Establish procedures and policies to establish a security assessment procedure.

PROCESS

Security Assessment and Authorization Policy and Procedures (CA-01)

The CISO in coordination with information system owners:

A. Develops, documents, and disseminates to information system owners:

1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and

B. Reviews and updates the current:

1. Security assessment and authorization policy as necessary; and

2. Security assessment and authorization procedures as necessary.

Security Assessment Policy

Security Assessments (CA-02)

A review of the College District's information security program for compliance with these standards will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program and designated by the College District's head or his or her designated representative(s).

The CISO must develop a security assessment plan. The security assessment will review the security controls and operation determining the extent to which the controls are implemented correctly and operate as intended. The assessment must be performed by individual(s) independent of the CISO. The results of the security assessment must be reported to the Chancellor/CEO

Information Exchange (CA-03)

The College District authorizes all connections from internal/organization information system to other information systems outside of organization through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.

Information resource owner must authorize all dedicated sustained connections from an information resource to external information resources through the use of interconnection security agreements. Document each interconnection interface, security requirements and information communicated. Agreements must be reviewed by CISO and updated as necessary. These connections will be included in the annual risk assessments.

Plan of Action and Milestones (CA-05)

The College District develops and updates, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Information resource owners in coordination with CISO must develop a plan of action including milestones to remediate deficiencies noted during security assessments and reduce or eliminate known vulnerabilities in the system in particular applying security patches and software updates.

Security Authorization (CA-06)

The College District authorizes the information system for processing before operations or when there is a significant change to the system. A senior organizational official, or their delegate, approves the authorization.

An Information resource owner is assigned to each information system. The information system owner must authorize the information resource for processing before commencing operations and ensures the security authorization is updated.

Continuous Monitoring (CA-07)

The College District monitors the security controls in the information system on an ongoing basis.

The CISO in coordination with information resource owners must develop a continuous monitoring strategy and implement continuous monitoring including metrics to be monitored along with monitoring methodology and response actions to the correlation of related security monitoring events.

Reporting the security and privacy status of the information systems to the Executive Vice Chancellor on an annual basis.

Penetration Testing (CA-08)

The College District conducts penetration testing at least biannually on external facing information systems.

The CISO coordinates with information system owners in the conduct of penetration testing to confirm vulnerabilities are corrected and access controls are in-place. The results of penetration testing are part of the security assessment.

Texas Government Code § 2054.516(a)(2) requires each state agency implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information to subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.

Agencies shall perform, or have performed, an external network penetration test every two years at minimum.

Internal System Connections (CA-09)

The College District has a procedure for authorizing internal information resource connections.

Information resource owner must authorize all dedicated sustained connections from an information resource to internal information resources. Document each interconnection interface, security requirements and information communicated. Connections must be reviewed by CISO and updated annually. These connections will be included in the annual risk assessments.