BLINN COLLEGE ADMINISTRATIVE REGULATIONS MANUAL

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

PURPOSE

Develop policies and procedures for risk assessment.

PROCESS

Risk Assessment Policy and Procedures (RA-01)

The College District

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

B. Reviews and updates the current:
   1. Risk assessment policy biennially; and
   2. Risk assessment procedures annually.

Risk Assessment Policy

Blinn College District shall perform and document risk assessments and make and document risk management decisions in compliance with 1 Texas Administrative Code §§ 202.25, 202.27. A state agency's security risk management plan may be excepted from disclosure under Texas Government Code § 2054.077(c) or Texas Government Code § 552.139.

Security Categorization (RA-02)

The College District

A. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
B. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
C. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Risk Assessment (RA-03)

The College District

A. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
B. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;
C. Documents risk assessment results in risk assessment report;
D. Reviews risk assessment results annually;
E. Disseminates risk assessment results to CISO, information owners and owners as appropriate; and
F. Updates the risk assessment annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Supply Chain Risk Assessment (RA-03 -1)

A. Assess supply chain risks associated with critical information system; and

B. Update the supply chain risk assessment biennially, when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

Vulnerability Scanning (RA-05)

The College District

A. Scans for vulnerabilities in the information system and hosted applications periodically and at least annually to confirm information systems are running the latest versions and when new vulnerabilities potentially affecting the system/applications are identified and reported;
B. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;
    4. Update vulnerabilities to be scanned prior to a new scan
C. Analyzes vulnerability scan reports and results from security control assessments;
D. Remediates legitimate vulnerabilities in coordination with information system owners and custodians in accordance with an organizational assessment of risk; and
E. Shares information obtained from the vulnerability scanning process and security control assessments with information system owners and custodians to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
    1. Affected system(s) may be isolated from the network.
F. Establish a public reporting channel through the infosec@blinn.edu email for receiving reports of vulnerabilities in organizational systems and system components

Risk Response (RA-07)

Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.