BLINN COLLEGE ADMINISTRATIVE REGULATIONS MANUAL

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

PURPOSE

Develop policies and procedures for system and communications protection.

PROCESS

System and Communications Protection Policy and Procedures (SC-01)

The College District

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

B. Reviews and updates the current:
   1. system and communications protection policy biennially; and
   2. System and communications protection procedures annually.

System and Communications Policy

Denial of Service Protection (SC-05)

The information system protects against or limits the effects of the network based denial of service attacks by employing: network firewalls, network traffic management techniques, network traffic logging; denial of service mitigation services.

Boundary Protection (SC-07)

The information system:

A. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
B. Implements subnetworks for publicly accessible system components that are physically or logically separated from internal College District networks; and
C. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the College District security architecture.

Transmission Confidentiality (SC-08)

The information system transmitting personally identifiable information, private health information and other protected and sensitive information must protect the confidentiality and integrity of transmitted information by encrypting transmission between the user and the information system using a minimum 128-bit encryption algorithm. Academic Technology maintains a departmental procedure defining the minimum encryption standards to be used.

Data loss prevention polices must be in place to identify, alert and block transmission of PII and other sensitive data from being shared based on documented risk analysis.

Academic Technology must configure information systems using the latest industry standard encryption protocols and technology to transmit confidential data.

Cryptographic Key Establishment and Management (SC-12)

The College District establishes and manages cryptographic keys for required cryptography employed within the information system. Key management should be automated when possible. Key management must protect the integrity of the keys and only be shared with those needing access to complete their job duties. Keys must be backed up and protected as part of the disaster management plan.

Academic Technology must administer and maintain cryptographic keys employed in client, network and enterprise systems in coordination with Administrative Computing and other College District departments.

Cryptographic Protection (SC-13)

The information system implements current generally accepted cryptographic standards in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Confidential, personally identifiable information, protected health information must be encrypted when stored on a portable storage device or transmitted over a public network.

Collaborative Computing Devices (SC-15)

The information system:

A. Prohibits remote activation of collaborative computing devices with the following exceptions: when an authorized employee or third party contractor is troubleshooting or maintaining the information system or a user is authorized to activate; and
B. Provides an explicit indication of use to users physically present at the devices.

Secure Name/Address Resolution Services (Authoritative Source) (SC-20)

The information system:

A. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
B. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.
C. The Network Systems manager or designee is responsible for maintaining the authoritative name resolution services.

Secure Name/Address Resolution Service (Recursive or Caching Resolver) (SC-21)

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

The Network Systems manager or designee is responsible for ensuring procedures are in place to maintain and protect the recursive name resolution service on the College District network.

Architecture and Provisioning for Name/Address Resolution Service (SC-22)

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

The Network Systems manager or designee is responsible for designing and maintaining a fault tolerant internal and external name/address resolution service.

Process Isolation (SC-39)

The information system maintains a separate execution domain for each executing process.

The information system owners must ensure the selection of operating systems supporting process isolation. Each process must execute in separate domains.