BLINN COLLEGE ADMINISTRATIVE REGULATIONS MANUAL

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

PURPOSE

Develop policies and procedures for personnel security.

PROCESS

Personnel Security Policy and Procedures (PS-01)

The College District

A. Develops, documents, and disseminates to information owners and custodians:
    1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
B. Reviews and updates the current:
    1. Personnel security policy biennially; and
    2. Personnel security procedures annually.

Personnel Security Policy

Position Risk Designation (PS-02)

The College District

A. Assigns a risk designation to all organizational positions;
B. Establishes screening criteria for individuals filling those positions; and
C. Reviews and updates position risk designations annually.

Position Screening (PS-03)

The College District

A. Screens individuals prior to authorizing access to the information system; and
B. Rescreens individuals according to Human Resources employment procedures.
C. All authorized users (including, but not limited to, Blinn College District personnel, temporary employees, and employees of independent contractors) of the District's information resources shall formally acknowledge that they will comply with the security policies and procedures of the District or they shall not be granted access to information resources. The method of acknowledgement is part of the required cyber security training which is conducted annually to maintain access to College District information resources.

Personnel Termination (PS-04)

The College District upon termination of individual employment:

A. Disables information system access within 24 hours;
B. Terminates/revokes any authenticators/credentials associated with the individual;
C. Conducts exit interviews that include a discussion of topics determined by Human Resources procedures;
D. Retrieves all security-related organizational information system-related property;
E. Retains access to organizational information and information systems formerly controlled by terminated individual; and
F. Notifies additional information owners within 48 hours.

Personnel Transfer (PS-05)

The College District

A. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
B. Initiates standard account modification procedures 48 hours;
C. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
D. Notifies additional information owners within 48 hours.

Access Agreements (PS-06)

The College District

A. Develops and documents access agreements for organizational information systems;
B. Reviews and updates the access agreements annually; and
C. Ensures that individuals requiring access to organizational information and information systems:
    1. Sign appropriate access agreements prior to being granted access; and
    2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or biennially.

Third Party Personnel Security (PS-07)

The College District

A. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
B. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
C. Documents personnel security requirements;
D. Requires third-party providers to notify information owners of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within 72 hours; and
E. Monitors provider compliance.

Personnel Sanctions (PS-08)

The College District

A. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
B. Notifies information system owners following Human Resources and Board Policy procedures.