BLINN COLLEGE ADMINISTRATIVE REGULATIONS MANUAL

SUBJECT: *Information Access Control*
EFFECTIVE DATE: March 1, 2020; amended September 19, 2023
BOARD POLICY REFERENCE: CS

PURPOSE

Establish procedures and policies for information systems access control.

PROCESS

User accounts (AC-1)

Employee accounts must be created based on information gathered and provided by the Human Resources department as part of the on-boarding process. Account creation request must be submitted and documented through the Academic Technology Help Desk system.

Student accounts must be created based on information gathered and provided by the Admissions department as part of the student's admissions application process. Account creation is based on student status in the student information system.

Other system accounts are created by information system owners in coordination with Academic Technology and Administrative Computing.

Account Management (AC-2 and (3))

Create and disable accounts according to Information Systems Identification and Authentication and Personnel Security administrative regulations, when in violation of organizational policy; or have been inactive for a period of time as defined in an Academic Technology departmental procedure.

Confidential information must be accessible only to authorized users. Information controls must be in place to restrict access to confidential information in its entirety to all users unless explicitly allowed by user account or access control group. Information resources assigned from one state organization to another or from a state organization to a contractor or other third party, at a minimum, must be protected in accordance with the conditions imposed by the providing state organization.

Access Enforcement (AC-3)

Each user account must be assigned a unique identifier. Each user must be authenticated before access to information system is granted.

Separation of Duties (AC-5)

User accounts and administrative accounts must be segregated and use of each must be used only to complete the required tasks with minimum level of rights. Production, test and development systems must be segregated either physically or logically. User accounts and underlying systems must be separated so as to prevent the co-mingling of data, accounts and access control.

Only when an application or system does not provide mechanisms for distributed administrative access can a shared system administrator account be used.

Shared system administrator accounts must be escrowed to provide shared access as needed to conduct business. Shared system administrator accounts must be changed when individuals knowing the password leaves employment or job duties change where they no longer administer the system or a contractor or vendor leaves or completes their work.

Least Privilege (AC-6)

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Unsuccessful Login Attempts (AC-7)

Enforce a limit of consecutive invalid logon attempts by a user during a defined time-period. Automatically: lock the account or node; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator as defined in a departmental procedure.

System Use Notification (AC-8)

Notifications must be placed on information systems login screens stating

- Unauthorized use is prohibited;

- Usage may be subject to security testing and monitoring;

- Misuse is subject to criminal prosecution; and

- Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

Permitted Actions without Identification or Authentication (AC-14)

A. Identify user actions that can be performed on the system without identification or authentication consistent with organizational missions and business functions; and
B. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

Remote Access (AC-17)

All remote access to information systems must be authorized by CISO. No remote access from outside the Blinn College District network will be provided via software or hardware without prior authorization. Remote access using Virtual Private Network (VPN) and Virtual Desktop Infrastructure (VDI) must require multifactor authentication.

Wireless Access (AC-18)

Wireless networks including IEEE 802.11 based WiFi, Bluetooth, infrared or other means to transmit information wirelessly must be configured with the minimum following restrictions.

1. Wireless Local Area Networks. Ensure that Service Set Identifiers (SSID) values are changed from the manufacturer's default setting. Some networks should not include organizational or location information in the SSID. Additional equipment configuration recommendations are included in the Wireless Security Guidelines.

2. Personal or sensitive information must only be transmitted via wireless networks and devices with encryption including mission critical information or sensitive personal information.

3. Wireless access points must not be connected to the Blinn College District network without prior authorization by Academic Technology. Personal wireless access points must not be connected to the Blinn College District network.

4. Wireless access network SSIDs must be segmented for employee, student and guest users. Network resource access restrictions must be placed on each SSID such that only required resources matching their usage needs are accessible.

5. All users must be authenticated.

Devices (AC-19)

Mobile computing and storage devices which process, store or transmit confidential information must be protected from unauthorized access by passwords or other personal authentication means. Any confidential information stored on mobile computing or storage device must be encrypted.

Transmission of confidential information between information resources and mobile computing devices must be encrypted.

Accessing college resources on a mobile device can enable remote wipe capabilities. This capability can be used in the case of loss of a device or to remove college data. Remote wipes can be initiated by device owner or authorized college personnel.

Mobile computing devices must be encrypted, patched and updated, protected with anti-virus/malware and if appropriate a personal firewall enabled.

External Systems (AC-20)

External information systems are information systems operated outside the Blinn College District network. External information systems must be reviewed by the CISO to ensure compliance with governing policies and laws. The terms and conditions must be reviewed as part of the procurement and legal review process. External system's controls must be compliant with TX-RAMP requirements throughout the contract period.

Publicly Accessible Content (AC-22)

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for nonpublic information and remove such information, if discovered.