

## **PURPOSE**

Establish procedures and policies for information systems access control.

## **PROCESS**

### **User accounts (AC-01)**

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 by the Human Resources department and documented through the 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 Information Technology Department.

### **Account Management (AC-02)**

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-03)**

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-05)**

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.

### **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.

### **Remote Access (AC-17)**

All remote access to information systems must be authorized by the Division Director of Information Technology and the Chief Information Security Officer (CISO). No remote access from outside the Temple College 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 Wi-Fi, 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 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 Temple College network without prior authorization by Information Technology department. Personal wireless access points must not be connected to the Temple College 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 resource and mobile computing devices must be encrypted.

**Subject:** Information Access Control (AC)

**Board Policy Reference:** CS (LOCAL) Information Security

---

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 Temple College network. External information systems must be reviewed by the Division Director of Information Technology and the Chief Information Security Officer (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.

\*If the Chief Information Security Officer (CISO) and the Division Director of Information Technology are the same individual, the coordination as indicated in the policy requires coordination with immediate supervisor.

- Temple College is responsible for IT regulatory compliance as specified by the Department of Education, the Texas Higher Education Coordinating Board, and the State of Texas Administrative Code (TAC202) for Information Technology. The IT policies include the specific guidance, requirements, and procedures in line with the regulatory and audit requirements.