Access Control Guideline

Purpose

The purpose of this guideline is to establish a minimum expectation with respect to access controls in order to protect data stored on computer systems throughout the Austin Peay University network.

Guideline

I. Overview

A. Austin Peay State University will control user access to information assets based on requirements of individual accountability, need to know, and least privilege.

B. Access to university information assets must be authorized and managed securely in compliance with appropriate industry practice and with numerous applicable legal and regulatory requirements (e.g., the Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, the Open Records Act of Tennessee, Gramm Leach Bliley Act, and identity theft laws).

C. University information assets include data, hardware and software technologies, and the infrastructure used to process, transmit, and store information.

1. Any computer, laptop, printer or device that an authorized user connects to the campus network is subject to this policy.
2. Guest, unauthenticated access may be provisioned commensurate with usage and risk.
3. Authorized users accessing university computing resources and network with their own personal equipment are responsible for ensuring the security and integrity of the systems they are using to establish access.

II. Access Controls

A. Access to information assets must be restricted to authorized users and must be protected by appropriate physical, administrative, and logical authentication and authorization controls.

B. Protection for information assets must be commensurate with the classification level assigned to the information.

C. Each computer system shall have an access control process that identifies and authenticates users and then permits access based on defined requirements or permissions for the user or user type.

D. All users of secure systems must be accurately identified, a positive identification must be maintained throughout the login session.

E. Access control mechanisms may include user IDs, access control lists, constrained user interfaces, encryption, port protection devices, secure gateways/firewalls, and host-based authentication.

III. User Identification, Authentication, and Accountability

A. User IDs:

1. The access control process must identify each user through a unique user identifier (user ID) account.
2. User IDs are assigned by the Austin Peay State University Office of Information Technology personnel.
3. Users must provide their user ID at logon to a computer system, application, or network.

B. Individual Accountability:

1. Individual accountability must be maintained.
2. Each and every user ID must be associated with an individual person who is responsible for its use.

C. Authentication:

1. Authentication is the means of ensuring the validity of the user identification.
2. All user access must be authenticated.
    a. The minimum means of authentication is a personal confidential password that the user must provide with each system and/or application logon.
    b. All passwords used to access information assets must conform to certain requirements relating to password composition, length, expiration, and confidentiality. Please refer Policy 4:039, Password Management for additional requirements.

IV. Access Privileges

A. Each user's access privileges shall be authorized on a need-to-know basis as dictated by the user's specific and authorized role.

B. Authorized access will be based on least privilege.

   1. This means that only the minimum privileges required to fulfill the user's role will be permitted.
   2. Access privileges must be defined so as to maintain appropriate segregation of duties to reduce the risk of misuse of information assets.
   3. Any access that is granted to data must be authorized by the appropriate data custodian.

C. Access privileges should be controlled based on the following criteria, as appropriate:

   1. Identity (user ID);
   2. Role or function;
   3. Physical or logical locations;
   4. Time of day/week/month;
   5. Transaction based access;
   6. Access modes such as read, write, execute, delete, create, and/or search.

D. Privileged access (e.g., administrative accounts, root accounts) must be granted based strictly on role requirements.

   1. The number of personnel with special privileges should be carefully limited.

V. Access Account Management

A. User ID accounts must be established, managed, and terminated to maintain the necessary level of data protection.

B. The following requirements apply to network logons as well as individual application and system logons, and should be implemented where technically and procedurally feasible:

   1. Account creation requests must specify access either explicitly or a role that has been mapped to the required access.
      a. New accounts created by mirroring existing user accounts must be audited against the explicit request or roles for appropriate access rights.
   2. Accounts must be locked out after five consecutive invalid logon attempts where feasible.

a. When a user account is locked out, it should remain locked out for a minimum of five minutes or until authorized personnel unlocks the account.

3. Systems housing or using restricted information must be configured in such a way that access to the restricted information is denied unless specific access is granted.
    a. Access to restricted information is never to be allowed by default.
4. Access must be revoked immediately upon notification that access is no longer required.
    a. Access privileges of terminated or transferred users must be revoked or changed as soon as possible.
    b. In cases where an employee is not leaving on good terms, the user ID must be disabled simultaneously with departure.
    c. Access for users who are on leaves of absence or extended disability should be suspended when feasible until the user returns.
5. User IDs will be disabled after a period of inactivity that is determined appropriate by the current business process.
6. All third party access (contractors, business partners, consultants, vendors) must be authorized and monitored.
7. Appropriate logging will be implemented commensurate with sensitivity/criticality of the data and resources.
    a. Logging of attempted access must include failed logons.
    b. Where practical, successful logons to systems with restricted information should be logged.
    c. Logs should be monitored and regularly reviewed to identify security breaches or unauthorized activity.
    d. Logs should be maintained for at least ninety days.
8. A periodic audit of secured systems to confirm that access privileges are appropriate must be conducted.
    a. The audit will consist of reviewing and validating that user access rights are still needed and are appropriate.

VI. Compliance and Enforcement

A. This guideline applies to all users of information resources including students, faculty, staff, temporary workers, vendors, and any other authorized users who are permitted access.

B. Persons in violation of this guideline are subject to a range of sanctions (determined and enforced by university management), including the loss of computer network access privileges, disciplinary action, dismissal from the institution, and legal action.

C. Some violations may constitute criminal offenses, per Tennessee and other local, and federal laws. The institution will carry out its responsibility to report such violations to the appropriate authorities.

VII. Exceptions

A. Documented exceptions to this policy may be granted by the Director of Information Technology Security based on limitations to risk and use.