EAST TENNESSEE STATE UNIVERSITY

Access Control	
Responsible Official: Chief Information Officer	Responsible Office: Information Technology Services

Policy Purpose

The Access Control Policy determines the settings used for limiting access to university computer systems and information stored on those systems. The controls listed provide guidance on account management and privilege assignments. The guidance defines the assignment of roles and associated business functions. Other controls include login time, screen saver requirements, and similar activity-based controls. This policy establishes a minimum expectation, with respect to access controls, in order to protect data stored on computer systems at East Tennessee State University (ETSU).

Policy Statement

I. Access Control Policy

Information Technology Services (ITS) shall develop, disseminate, and periodically review and/or update formal, documented University policies for Access Control and procedures to facilitate the implementation of the Access Control best practices.

II. General

A. ETSU 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 applicable legal and regulatory requirements (e.g., Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, Open Records Act of Tennessee, Gramm Leach Bliley Act, and identity theft laws).

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

1. Guest/unauthenticated access may be provisioned commensurate with usage and risk.

2. 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.

III. 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 confidentiality of the information.

C. Each computer system shall have an automated 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, and actions must be linked to specific users.

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.

IV. 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 Information Technology Services (ITS).
3. Users must provide their user ID at logon to a computer system, application, or network.

B. Individual Accountability

1. Each 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 secret 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.

V. 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 (i.e., administrative accounts, root accounts) must be granted based strictly on role requirements.

VI. 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 for a role that has been mapped to the required access.
   2. Accounts must be locked out after a specified number of consecutive invalid logon attempts and remain locked out for a specified amount of time or until authorized personnel unlock the account.
   3. User interfaces into secure systems must be locked after a specified system/session idle time.
   4. Systems housing or using restricted information must be configured so that access to the restricted information is denied unless specific access is granted.
   5. Access must be revoked immediately upon notification that access is no longer required or authorized.
      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.
   6. User IDs will be disabled after a period of inactivity that is determined appropriate by the current business process.
   7. All third party access (contractors, business partners, consultants, vendors) must be authorized and monitored.
   8. Appropriate logging will be implemented commensurate with sensitivity/criticality of the data and resources.
      a. Logging of attempted access must include failed logons.

   b. Logs should be monitored and regularly reviewed to identify security breaches or unauthorized activity.
   c. Logs should be maintained for a specified period of time.

9. A periodic audit of secured systems to confirm that access privileges are appropriate must be conducted. The audit will consist of reviewing and validating that user access rights are still needed and are appropriate.

VII. Compliance and Enforcement

A. This policy 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 policy 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 University will carry out its responsibility to report such violations to the appropriate authorities.

VIII. Exceptions

Documented exceptions to this policy may be granted by the Chief Information Officer in consultation with the Office of Legal Counsel.

Authority: (None)

Definitions

Policy History

Effective Date:
Revision Date:

Procedure (s)

I. Account Access Procedures

The University applies these Account Management practices to all accounts on ITS systems, including accounts used by vendors and third parties.

1. ITS Identifies and selects the following types of information system accounts to support the university missions/business functions:
   a. Employees
   b. Students
   c. Alumni
   d. Guests
2. Assigns account manager/sponsors for information system accounts;
3. Establishes conditions for group and role membership;

4. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
5. A University Sponsor approves the request to create information system accounts;
6. Creates, enables, modifies, disables, and removes information system accounts with automated controls.
7. Monitors the use of information system accounts;
8. Notifies account managers:
    a. When accounts are no longer required;
    b. When users are terminated or transferred; and
    c. When individual information system usage or need-to-know changes;
9. Authorizes access to the information system based on:
    a. A valid access authorization;
    b. Intended system usage; and
    c. Other attributes as required by the university or associated missions/business functions;
10. Reviews accounts for compliance with account management requirements yearly and
11. Establishes a process for reissuing shared/group account credentials when individuals are removed from the group.
12. Employs automated mechanisms to support the management of information system accounts.
13. Disables temporary and emergency accounts after 30 days.
14. Disables inactive accounts after 210 days of inactivity.
15. Audits account creation, modification, enabling, disabling, and removal actions, and notifies the system owner.
16. Require that users log out when they are no longer need the active session.
17. implements dynamic privilege management capabilities when this capability is required.
18. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
19. Monitors privileged role assignments and removes access when privileged role assignments are no longer appropriate.
20. Creates accounts and access dynamically when appropriate.
21. Disables accounts of users posing a significant risk within one hour of discovery of the risk.

II. Information Flow Enforcement

The flow of sensitive information between systems is controlled and/or monitored through technical (network firewalls, intrusion prevention, data loss prevention) means.

III. Separation Of Duties

ETSU enforces separation of duties to aide in the prevention of both fraud and errors from a lack of quality control. The person requesting a change in access should not be the person who plans and then implements the change.

IV. Least Privilege

ETSU implements least privilege by limiting the rights/privileges or accesses assigned to users to enable performance of specified tasks while adequately mitigating risk to the organization, individuals, and other organizations.

V. Unsuccessful Login Attempts

ETSU defines the maximum number of consecutive invalid user login attempts, a time-period in which the consecutive invalid access attempts occur, and a defined response to be taken should this maximum number of invalid login attempts occur during the defined time-period.

1. Enforces a limit of 10 consecutive invalid logon attempts by a user during a one-hour period and
2. Automatically locks the account/node for 1 hour.
3. The information system has the ability to purge/wipe information from University managed mobile devices after ten consecutive, unsuccessful device logon attempts.

VI. System Use Notification

ETSU's information system displays an approved system use notification message before granting system access. The message displayed includes privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. All users must accept the terms in this notification message prior to using any ETSU computing resources.

VII. Previous Logon (Access) Notification

With regard to both traditional logons to information systems and general access to information systems that occur in various system configurations, the information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

VIII. Concurrent Session Control

The information system limits the number of concurrent sessions for each system account as defined by the system owner.

IX. Session Lock

The information system:

1. Prevents further access to the system by initiating a session lock after one hour of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

X. Session Termination

Session timeout represents an event occurring when a user does not perform any action on a web site during a period of time. The lack of action changes the status of the user session to 'invalid'. The information system automatically terminates a user session after one hour of inactivity.

XI. Remote Access

ETSU defines standards for connecting to the University's network from any host. These standards are designed to minimize the potential exposure to the University from damages which may result from unauthorized use of University resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical University internal systems, etc.

The University:

1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.
2. Authorizes remote access to the information system prior to allowing such connections.
3. The information system monitors and controls remote access methods.
4. The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
5. The information system routes all remote accesses through the University primary firewall managed by ITS.
6. ETSU ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.
7. ETSU provides the capability to expeditiously disconnect or disable remote access to the information system following one hour of idle time.

XII. Wireless Access

ETSU defines standards for connecting to the University's wireless network from any host. These standards are designed to minimize the potential exposure to the University from damages which may result from unauthorized use of University resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical University internal systems, etc.

The University:

1. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
2. Authorizes wireless access to the information system prior to allowing such connections.
3. The information system protects wireless access to the system using authentication of users and encryption.

4. ETSU disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.
5. ETSU identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.
6. ETSU selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

XIII. Access Control For Mobile Devices

Procedures for requirements regarding access control for mobile devices will mitigate risk from malicious or otherwise compromised devices to the University's information system. The university:

1. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
2. Authorizes the connection of mobile devices to organizational information systems.

XIV. Use Of External Information Systems

The University establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

1. Access the information system from external information systems; and
2. Process, store, or transmit organization-controlled information using external information systems.

The University:

3. Verifies the implementation of required security controls on the external system as specified in the information security policy and security plan; or
4. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.
5. Controls the use of organization-controlled portable storage devices by authorized individuals on external information systems.
6. Controls the use of network accessible storage devices in external information systems.

XV. Data Mining Protection

This control establishes the process of securing Analysis Services that occur at multiple levels. Each instance of Analysis Services and its data sources must be secure to make sure that only authorized users have read or read/write permissions to selected dimensions, mining models, and data sources, and to prevent unauthorized users from maliciously compromising sensitive business information. The University employs data mining prevention and detection techniques to adequately detect and protect against data mining.

Procedure History

Effective Date:

Revision Date:

Related Form(s)

Scope and Applicability

Check those that apply to this policy and identify proposed sub-category.

	Governance	
	Academic	
	Students	
	Employment	
X	Information Technology	Access
	Health and Safety	
	Business and Finance	
	Facilities and Operations	
	Advancement	