Access Control Data Security Policy	
Responsible Official: Chief Information Officer	**Responsible Office**: Information Technology Services

Policy Purpose

This Policy specifies the data security control procedures used for limiting access to East Tennessee State University (ETSU) computer systems and the information stored on those systems

Policy Statement

Access controls are necessary to ensure only authorized users can obtain access to ETSU's information and systems. Information Technology Services (ITS) access control security procedures provide guidance on account management and privilege assignments.

This policy applies to all ETSU users of information resources including students, faculty, staff, temporary workers, contractors, vendors, and any other authorized users that connect to ETSU servers, applications, or network devices that contain or transmit ETSU data.

I. Access Control Policy

ITS shall develop, disseminate, and periodically review and/or update formal, documented ETSU 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 ETSU information assets must be authorized and managed securely in compliance with appropriate industry practice and with applicable legal and regulatory requirements.

C. ETSU 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 ETSU 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 technical (including logical authentication and authorization) controls.
B. Protection of 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, but are not limited to, 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. 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 for all systems storing ETSU data are a personal secret password and a secondary authentication provided by the user.
      b. During prolonged sessions, re-authentication must occur every 12 hours. Re-authentication must occur after no more than 30 minutes of inactivity.
      c. All passwords used to access information assets must meet the established minimum criteria defined in the ETSU Strong Password Requirement Policy.

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 least 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. Access to data must be authorized by the appropriate data custodian.
4. Administrative, root, or other privileged account access must be granted strictly on role requirements.

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.

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 via 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 amount of 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 users must be revoked or changed as soon as possible after the last day of work date or upon notification from Human Resources, Legal Counsel, or the Chief Information Officer.
    b. Access privileges of transferred employees should be reviewed to confirm ongoing need for current access privileges.
        (a) In the event that job duties require temporary overlapping privileges, timely review of that access must be conducted.

c. In cases where an employee is terminated for cause, the user ID must be disabled simultaneously with or prior to departure.

6. User IDs will be disabled after 90 days of inactivity.
7. All third-party access (contractors, business partners, consultants, vendors) must be authorized, monitored, and subject to least privilege.
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, contractors, 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 ETSU 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 federal laws. ETSU 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.

Authority: T.C.A § 49-8-203, National Institute of Standards and Technology (NIST) 800-53. Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, Open Records Act of Tennessee, Gramm Leach Bliley Act

Previous Policy: TBR Access Control: 1.08.03.00

Defined Terms

Information System:	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Policy History

Effective Date

Initial: May 13, 2019

Revised: February, 2022

Procedure

I. Access Management

Establishes the steps necessary to formalize the process of requesting, granting, administering, and terminating accounts. The ETSU shall apply these Account Management practices to all accounts on ITS systems, including accounts used by vendors and third parties:

A. Identify and select the following types of information system accounts to support the ETSU missions/business functions:
   1. Employees
   2. Students
   3. Alumni
   4. Guests
B. Assign account manager/sponsors for information system accounts.
C. Establish conditions for group and role membership.
D. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
E. Requires approval by an ETSU sponsor for requests to create information system accounts.
F. Create, enable, modify, disable, and remove information system accounts with automated controls. Manual controls are discouraged and should be applied in a reasonable time.
G. Monitor the use of information system accounts.
H. Notify account managers:
   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual information system usage or need-to-know changes.
I. Authorize access to the information system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the ETSU or associated missions/business functions.
J. Review accounts for compliance with account management requirements bi-annually.
K. Employ automated mechanisms to support the management of information system accounts.

L. The information system automatically disables temporary and emergency accounts after 30 days.
M. The information system automatically disables inactive accounts after 90 days of inactivity.
N. The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies the system owner.
O. Require that users log out when they no longer need the active session.
P. The information system implements dynamic privilege management capabilities when this capability is required.
Q. Establish and administer privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.
R. Monitor privileged role assignments.
S. Remove access when privileged role assignments are no longer appropriate.
T. Disable 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.

A. Enforces a limit of 10 consecutive invalid logon attempts by a user during a one-hour period and
B. Automatically locks the account/node for 1 hour.
C. The information system has the ability to purge/wipe information from ETSU 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)

With regard to both traditional logons to information systems and general access to information systems that occur in various system configurations, the information system logs 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:

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

The ETSU:

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

The ETSU:

A. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
B. Authorizes wireless access to the information system prior to allowing such connections.
C. The information system protects wireless access to the system using authentication of users and encryption.
D. ETSU disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.
E. ETSU identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.
F. 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 ETSU's information system.

The ETSU:

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 ETSU 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:

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

The ETSU:

C. Verifies the implementation of required security controls on the external system as specified in the information security policy and security plan; or

D. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.
E. Controls the use of organization-controlled portable storage devices by authorized individuals on external information systems.
F. 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 ETSU employs data mining prevention and detection techniques to adequately detect and protect against data mining.

Procedure History

Effective Date

Initial: May 13, 2019

Revised: February, 2022

Related Form(s)

Scope and Applicability

Primary: Information Technology

Secondary: