EAST TENNESSEE STATE UNIVERSITY

Access Control Data Security

Policy Effective Date: 5/13/2019 • **Policy Revised Effective Date:** 5/10/2022; 1/13/2025
Procedures Effective Date: 5/13/2019 • **Procedures Revised Effective Date:** 5/10/2022; 1/13/2025

Policy Name: Access Control Data Security

Policy Purpose

This policy specifies the data security control procedures used for limiting access to ETSU computer systems and the information stored on those systems.

Applicability

This policy is applicable to all ETSU users of information resources including students, employees, contractors, vendors, and any other authorized users that connect to ETSU servers, applications, or network devices that contain, utilize, or transmit ETSU data.

Responsible Official, Office, and Interpretation

Information Technology Services and Information Technology Council are responsible for the review and revision of this policy. For questions about this policy, please contact Information Technology Services. The Chief Information Officer in consultation with the Office of University Counsel, has the final authority to interpret this policy.

Defined Terms

A defined term has a specific meaning within the context of this policy.

Access Control

A data security process that determines who can access an institution's resources and data, and under what conditions. Access controls are necessary to ensure that only authorized users obtain access to information and information systems.

Authentication

The process of verifying the validity of a user's identification before granting access to a system or resource.

Information System

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

Least Privilege

An information security concept that limits access to only what is required for the user to perform their role or complete a task.

Policy Name: Access Control Data Security

Policy

ETSU will control user access to information assets based on requirements of individual accountability, need to know, and least privilege. ETSU information assets include data, hardware, software technologies, and the infrastructure used to process, transmit, and store information. Access to ETSU information assets must be authorized and managed securely in compliance with appropriate industry practice, applicable legal and regulatory requirements, and the security framework adopted in ETSU's Information Security Policy. Guest / unauthenticated access may be provisioned commensurate with usage and risk.

Authorized users accessing ETSU computing resources and network with personal equipment are responsible for ensuring the security and integrity of the systems they are using to establish access; ITS reserves the right to block out-of-support and unpatched systems from the network. Authorized users are responsible for the protection of their passwords and secondary authentication devices and applications.

1. Access Controls.

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. Protection of information assets must be commensurate with the sensitivity and confidentiality of the information.

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

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.

Access control mechanisms may include, but are not limited to, user IDs, passwords, multi-factor authentication hardware and applications, biometrics, location, day and time, velocity, IP reputation, access control lists, constrained user interfaces, encryption, port protection devices, secure gateways/firewalls, and host-based authentication.

All systems on the ETSU network must employ multi-factor authentication. Failure to do so dramatically reduces cyber liability insurance coverage.

2. User Identification, Authentication, and Accountability.

2.1. User IDs.

The access control process must identify each user through a unique user identifier (user ID) account. User IDs are assigned by Information Technology Services. Users must provide their user ID at logon to a computer system, application, or network. Every user ID must be associated with an individual person, who is responsible for its use.

2.2. Authentication.

All user access must be authenticated. The minimum means of authentication for all systems storing ETSU data are a personal secret password and a secondary authentication provided by the user.

During prolonged sessions, re-authentication must occur at the minimum interval specified in relevant laws, regulations, and the chosen cybersecurity framework. Re-authentication must occur following the minimum period of inactivity as required by relevant laws, regulations, and the chosen cybersecurity framework.

All passwords used to access information assets must meet minimum criteria defined in the ETSU Strong Password Requirement Policy.

3. Access Privileges.

Each user's access privileges shall be authorized on a need-to-know basis as dictated by the user's specific and authorized role. Authorized access will be based on least privilege principles. Access privileges must be defined to maintain appropriate segregation of duties to reduce the rise of misuse of information assets. Access to data must be authorized by the appropriate data owner. Administrative, root, or other privileged account access must be granted strictly on role requirements.

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

3.1. Identity (user ID);

3.2. Role or function;

3.3. Physical or logical location;

3.4. Time of day, week, month;

3.5. Transaction based access; and

3.6. Access modes such as read, write, execute, delete, create, and/or search.

4. Access Account Management.

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

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

4.1. Account creation requests must specify access either explicitly or via a role that has been mapped to the required access.

4.2. 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.

4.3. User interfaces into secure systems must be locked after a specified amount of system/session idle time.

4.4. Systems housing or using restricted information must be configured so that access to the restricted information is denied unless specific access is granted.

4.5. Access must be revoked immediately upon notification that access is no longer required or authorized.

4.6. 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 the Office of Human Resources, the office of University Counsel, the President or their designee, or the Chief Information Officer or their designee.

4.7. Access privileges of transferred employees should be reviewed to confirm ongoing need for current access privileges.

4.8. In the event that job duties require temporary overlapping privileges, timely review of that access must be conducted.

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

4.10. User IDs will be automatically disabled after 90 days of inactivity.

4.11. All third-party access (contractors, business partners, consultants, vendors) must be authorized, monitored, and subject to least privilege principles.

Appropriate logging will be implemented commensurate with sensitivity/criticality of the data and resources. Logging of attempted access must include failed logons. Logs should

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

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.

5. Separation of Duties.

ETSU enforces separation of duties to aid 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.

6. 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.

7. 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.

8. Remote Access.

ETSU defines standards for connecting to the ETSU network from any host. These standards are designed to minimize the potential exposure to damages which may result from unauthorized use of ETSU resources. Damages include but are not limited to the loss of sensitive or confidential data, intellectual property, damage to public image, and damage to critical ETSU internal systems. ETSU:

8.1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

8.2. Authorizes remote access to the information system prior to allowing such connections.

8.3. Monitors and controls remote access methods.

8.4. Implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

8.5. Routes all remote accesses through the ETSU primary firewall managed by Information Technology Services.

8.6. Ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

8.7. Provides the capability to expeditiously disconnect or disable remote access to the information system following 15 minutes of idle time.

9. Wireless Access.

ETSU defines standards for connecting to ETSU's wireless network from any host. These standards are designed to minimize the potential exposure to damage which may result from unauthorized use of ETSU resources. Damages include but are not limited to the loss of sensitive or confidential data, intellectual property, damage to public image, and damage to critical ETSU internal systems. ETSU:

9.1. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

9.2. Authorizes wireless access to the information system prior to allowing such connections.

9.3. Protects wireless access to the system using authentication of users and encryption.

9.4. Disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.

9.5. Identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

9.6. Selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

10. Access Control for Mobile Devices.

Requirements regarding access control for mobile devices will mitigate risk from malicious or otherwise compromised devices to ETSU's information systems. 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.

11. Use of External Information Systems.

ETSU establishes terms and conditions, consistent with 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.

ETSU verifies the implementation of required security controls on the external system as specified in the information security policy and security plan or as documented in the risk memo resulting from security review; or retains approved information system connection or processing agreements with the organizational entity hosting the external information system. ETSU controls the use of organization-controlled portable storage devices by authorized individuals on external information systems. ETSU controls the use of network accessible storage devices in external information systems.

12. 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. ETSU employs data mining prevention and detection techniques to adequately detect and protect against data mining.

13. Compliance and Enforcement.

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. 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.

14. Exceptions.

Documented exceptions to this policy may be granted by the Chief Information Officer or their designee.

Procedures

1. Access Management.

ETSU will apply these account management practices to all accounts on ITS systems, including accounts used by vendors and third parties:

1.1. Identify and select the following types of information system accounts to support the ETSU mission/business functions: students, employees, contractors, vendors, and any other authorized users.

1.2. Assign account manager/sponsors for information system accounts.

1.3. Establish conditions for group and role membership.

1.4. 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.

1.5. Require approval by an ETSU sponsor for requests to create information system accounts.

1.6. Create, enable, modify, disable, and remove information system accounts with automated controls. Manual controls are discouraged and should be applied in a reasonable time.

1.7. Monitor the use of information system accounts.

1.8. Notify account managers:

1.8.1. When accounts are no longer required;

1.8.2. When users are terminated or transferred; and

1.8.3. When individual information system usage or need-to-know changes.

1.9. Authorize access to the information system based on:

1.9.1. A valid access authorization;

1.9.2. Intended system usage; and

1.9.3. Other attributes as required by ETSU or associated mission/business functions.

1.10. Review accounts for compliance with account management requirements bi-annually.

1.11. Employ automated mechanisms to support the management of information system accounts.

1.12. The information system automatically disables temporary and emergency accounts after 30 days.

1.13. The information system automatically disables inactive accounts after 90 days of inactivity.

1.14. The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies the system owner.

1.15. Require that users log out when they no longer need the active session.

1.16. The information system implements dynamic privilege management capabilities when this capability is required.

1.17. Establish and administer privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles.

1.18. Monitor privileged role assignments.

1.19. Remove access when privileged role assignments are no longer appropriate.

1.20. Disable accounts of users posing a significant risk within one hour of discovery of the risk.

2. Unsuccessful Login Attempts.

Five consecutive invalid logon attempts by a user during a one-hour period automatically locks the account/node for 15 minutes. The information system has the ability to purge/wipe information from ETSU managed mobile devices after 10 consecutive, unsuccessful device logon attempts.

3. Session Lock.

The information system: (1) Prevents further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user; and (2) retains the session lock until the user re-establishes access using established identification and authentication procedures.

4. Session Termination.

Session timeout represents an event occurring when a lack of user action changes the status of the user session to "invalid". The information system automatically terminates a user session after 15 minutes of inactivity.

Policy Name: Access Control Data Security

Applicable Forms and Websites

N/A

Authority and Revisions

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

The ETSU Board of Trustees is charged with policy making pursuant to TCA § 49-8-203, et seq. On March 24, 2017, the Board delegated its authority to ETSU's President to establish certain policies and procedures for educational program and other operations of the University, including this policy. The delegation of authority and required process for revision to this policy can be found on the Policy Development and Rule Making Policy webpage.

To suggest a revision to this policy, please contact the responsible official indicated in this policy. Before a substantive change to the policy section may take effect, the requested changes must be: (1) approved by the responsible office; (2) reviewed by the Office of University Counsel for legal sufficiency; (3) posted for public comment; (4) approved by either Academic Council or University Council; and (5) approved by ETSU's President.