THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: AC-001-Access Control	
Version 8	**Effective Date: 04/18/2016**

Responsible Office: Office of Cybersecurity	Last Review: 08/18/2022 Next Review: 08/18/2024
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

Access controls are designed to minimize potential exposure to the UTHSC (University of Tennessee Health Science Center) resulting from unauthorized use of Information Technology (IT) Resources and to preserve and protect the confidentiality, integrity, and availability of UTHSC networks, systems, and applications. This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but is not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

Scope

This standard applies to members of the UTHSC community who have a need to access UTHSC IT Resources.

Definitions

Confidentiality Integrity Availability (C-I-A) – The protection level based on classification ratings in the areas of confidentiality, integrity, or availability per GP-002-Data & System Classification

Information Technology (IT) Resources – The collection of data and technology that supports the achievement of organizational goals. IT Resources include hardware, software, vendors, users, facilities, data systems, and data.

Principle of Least Privilege – a given user account should be given only those privileges needed for it to complete its task.

Responsibilities

Chief Information Officer (CIO) or designee is responsible for the overall Identification & Authentication (IA) program at UTHSC and ensures that the program is developed, documented, and disseminated to appropriate UTHSC entities in accordance with university policies.

Chief Information Security Officer (CISO) or designee is responsible for overseeing the IA program and consults with system owners to ensure effective procedures are implemented.

Data Owner or designee is responsible for approving requests for additions, changes, and deletions of access rights and privileges to data or information for individual users. The Data Owner will forward the approved requests to the system custodian for implementation.

System Custodian is responsible for the day-to-day administration of the system including the creation and management of system access accounts for authorized users.

UTHSC-ITS is responsible for creating the UTHSC authenticator that is based on the NetID and password for all members of the UTHSC community.

UTHSC-ITS is responsible for implementing the approved access rights and permission requests for all users to UTHSC IT Resources.

UTHSC Community given access to UTHSC IT Resources, share responsibility for ensuring the appropriate security of information and addressing security lapses or breaches. Any observed violation of the Information Security Program must be reported.

Standard

User Access

1. Access to UTHSC IT Resources (e.g., data, systems, services, and networks) not categorized as a C-I-A zero (0) per GP-002-Data & System Classification must be documented and limited to authorized persons whose job responsibilities require access, as determined by the Data Owner or their delegate.
2. Access to UTHSC IT Resources (e.g., data, systems, services, and networks) not categorized as a C-I-A zero (0) per GP-002-Data & System Classification, requires individual authentication to obtain access to such resources to protect from unauthorized use.
3. Each UTHSC IT Resource must have a designated Data Owner who is responsible for overseeing, directing, and approving access to the system.

   a. The Data Owner, or delegate must hold a position of authority within UTHSC allowing the Data Owner, or delegate to approve all requests for access to the system.

4. Each UTHSC IT Resource must have at least one individual serving in the role of system custodian.
5. Requests for access rights and privileges to be granted, changed, or revoked must be made in writing to the Data Owner.
6. At regular intervals, System custodians and Data Owners will execute a formal documented process to review users' access rights.
7. Failure to comply with these standards will result in a loss of access or other disciplinary actions, up to and including termination.
8. Any anomalies found will be handled by the Security Incident Response Team in accordance with IR-001-Security Incident Response.

Administrative Access

1. Access rights and privileges to UTHSC IT Resources not categorized as a C-I-A zero (0) will be granted following the principles of least privilege and need to know. These access rights and privileges will be restricted and controlled, with documented authorization.
2. The allocation of special elevated (privileged) access rights (i.e., local administrator, domain administrator, super-user, root access) will be restricted and controlled, and documented authorization provided by the Data Owner, to the system's custodian.

Physical Access

1. Access to a physical location of IT Resources is restricted to authorized personnel having responsibility for installing or maintaining assets in these locations. Others requiring access are escorted and supervised by authorized personnel.
2. All entry points affording access to physical location of IT Resources are locked at all times.
3. Access to physical locations of IT Resources will be restricted by key, code, or electronic card. An auditable process for issuing keys, codes, and/or cards needs documentation.
4. Physical locations of IT Resources are continuously monitored by surveillance equipment.

Remote Access

1. Remote access to UTHSC IT Resources must have documented approval from the Owner of the UTHSC IT Resource.
2. Remote access control procedures must provide appropriate safeguards through documented identification, authentication, and encryption techniques. Direct log-on to campus UTHSC IT Resources from off-campus locations is not allowed. A remote user must first authenticate to an authorized campus remote access service with strong encryption before logging into a campus computer. This restriction does not apply to authenticated user access to web applications or to systems designed for public access.
3. A list of authorized campus remote access services is located at https://uthsc.edu/its/cybersecurity/remote-access.php.
4. Any device and/or network connected remotely to the UTHSC network is subject to the policies, standards, and practices that apply to UTHSC-owned equipment, i.e., devices must be configured to comply with all UTHSC Security Policies and must accept any Network Access Control agents required for enforcement of these policies and standards.
    a. All computers connected to UTHSC internal networks remotely must use up-to-date anti-virus software.
    b. All computers connected to UTHSC internal networks remotely must have the latest operating system security patches applied.
5. AC-001.04-VPN Access provides more specific requirements regarding the use of UTHSC's VPN for remote access. Information about UTHSC's VPN can be found on the VPN website.

References

1. AC-001-Access Control
2. AC-001.04-VPN Access
3. IR-001-Security Incident Response
4. GP-002-Data & System Classification
5. AC-002.02-Password Management and Complexity
6. PE-001-Physical Security of Information Resources and Related Facilities