THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: SC-002-System and Communication Protections	
Version 6	**Effective Date: 03/17/2018**

onsible Office: Office of Cybersecurity	Last Review: 01/25/2023 Next Review: 01/25/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

This standard establishes the system and communications protection for information systems supporting the UTHSC Computing and Communication environment. 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 the security of UTHSC IT Resources in the form of electronic communications, stored data, and electronic communications resources used to transmit, store, and process such data.

Definitions

IT Resource – any data, device, or other component of the information environment that supports information-related activities. Assets generally includer hardware (e.g., servers and switches), software (e.g., mission critical applications and support systems) and information.

Responsibilities

Information Technology Services (ITS) is responsible for implementing the security controls necessary to protect IT Resources.
Office of Cybersecurity is responsible for the assessment of security controls necessary to protect IT Resources and work with ITS in the implementation of those controls based on risk assessments.
UTHSC Workforce is responsible for adhering to this standard and the security controls set for in it.

Standard

UT Health Science Center: SC-002-System and Communication Protections	
Version 6	**Effective Date: 03/17/2018**

1. UTHSC will protect the confidentiality, integrity, and availability of IT Resources including data residing within these IT Resources and the communications among these IT Resources and with systems external to the UTHSC.
2. User functionality (including user interface services) shall be separated from information system management functionality in its systems.
3. Unauthorized and unintended information transfer via shared system resources is prohibited.
4. UTHSC shall take preventive measures to protect against or limit the effects of denial-of-service attacks.
5. UTHSC shall implement boundary protection. This protection shall address the external boundary as well as key internal boundaries, which shall be identified in the system security plan.
   a. Publicly accessible UTHSC IT Resources are to be located on separate sub-networks from internal networks.
   b. There will be no public access to the UTHSC internal network.
   c. Interfaces, interconnects, and their protection mechanisms to external networks shall be managed, monitored, and documented.
   d. The number of external network connections shall be limited.
   e. By default, the principle to deny traffic shall be implemented.
6. UTHSC shall terminate network connections at the end of the session or after a period of inactivity for remote sessions.
7. The integrity and confidentiality of UTHSC data and information with a level 3 classification ranking determined in GP-002-Data & System Classification shall be protected with encryption during transmission that meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation.
8. UTHSC shall provide Domain Name System (DNS) services that:
   a. Use encryption of all DNS services, when supported.
   b. Process name/address resolution requests from internal clients only with internal DNS servers.
   c. Process name/address resolution information requests from external clients only with external DNS servers.
   d. Provide fault-tolerant name/address resolution service for all information systems.
   e. Provide mechanisms to protect the authenticity of communications sessions.
9. Failure to comply with these standards should follow GP-001.04-Information Security Violations recommendations.

References

1. IT0135 - System and Information Integrity
2. GP-002-Data & System Classification
3. GP-001.04-Information Security Violations
4. National Institute of Standards and Technology (NIST) publication FIPS 140-2