THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

| UT Health Science Center:<br>SC-002-System and Communication Protections | |
|---|---|
| Version 5 | Effective Date: 03/17/2018 |

| | |
|---|---|
| Responsible Office: Office of Cybersecurity | Last Review: 03/27/2020<br>Next Review: 03/27/2022 |
| Contact: Chris Madeksho | Phone: 901.448.1579<br>Email: mmadeksh@uthsc.edu |

## Purpose

This standard establishes the system and communications protection for information systems supporting the UTHSC Computing and Communication environment.

## 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.

## Standard

1. UTHSC will protect the confidentiality, integrity, and availability of UTHSC IT Resources including data residing within these UTHSC IT Resources and the communications among these UTHSC 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 shall be prevented.
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 classification ranking of 3 in any area during transmission shall be protected with encryption 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 may result in a loss of access or other disciplinary actions, up to and including termination

## References

1. UTSA IT Policy [IT0135] System and Information Integrity
2. GP-002-Data & System Classification
3. Human Resources Policy 0525
4. National Institute of Standards and Technology (NIST) publication FIPS 140-2