THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: SC-001-Network Security	
Version 4	**Effective Date: 03/17/2016**

Responsible Office: Office of Cybersecurity	Last Review: 02/27/2023 Next Review: 02/27/2025
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

To specify the authority for UTHSC network infrastructure access, implementation, maintenance, operations, and change in the UTHSC network infrastructure. 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 all UTHSC members of the UTHSC Community and others making use of UTHSC network services.

Definitions

Network - Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Responsibilities

The **Vice Chancellor for Information Technology/CIO** approves Network Service Providers.

It is the responsibility of the **Network Service Provider** to provide network services that exceed or meet the security requirements of UTHSC Information Security Program.

Network Services provided by external entities (contracted Network Service Providers) must be formalized via an executed contract and/or service level agreement that include security requirements that exceed or meet those of the UTHSC Information Security Program.

Standard

1. Formally approved Network Service Providers and approved IT Staff are the only entities in UTHSC authorized to:
   a. Implement, change, remove, monitor, and operate UTHSC network infrastructure. This encompasses any and all essential network devices and components such as, but not limited to, cabling, hubs, switches, routers, network firewalls, intrusion detection and prevention devices, and wireless access points.
   b. Offer alternate methods of network access, access to network resources, and virtual private networks (VPNs).
   c. Offer or delegate network infrastructure services such as, but not limited to, DHCP and DNS.
   d. Assign and manage the network Internet Protocol (IP) address space.
   e. Monitor, analyze, and manage the security, utilization, and traffic patterns of the UTHSC network and network resources.
   f. Use tools to capture network traffic for diagnostic purposes.
   g. Inspect network traffic to confirm malicious or unauthorized activity that may harm UTHSC network or devices connected to the network. Such activity shall be limited to the least perusal of contents required to resolve the situation. User consent is not required for these routine-monitoring practices.
   h. Block and/or modify any network traffic deemed problematic or malicious affection of the integrity, availability, and confidentiality of UTHSC network.
2. All network-connected equipment must be configured to a specification consistent with Network Service Provider requirements.
3. All hardware connected to the network is subject to Network Service Provider network management and monitoring standards.
4. The network infrastructure supports a well-defined set of approved networking protocols.
5. All access to the UTHSC network must be authenticated.
6. No unsecured access points are allowed on UTHSC network.
7. Vendor access to network resources must be coordinated with the network service provider in collaboration with the Office of Cybersecurity.
8. Exceptions to this practice should be requested using the process outlined in

GP-001.02-Security Exceptions and Exemptions to ITS Standards Practices & Controls

9. Failure to comply with this policy could result in loss of network access by the offending device and/or disciplinary action for the offender(s).

References

1. UTHSC Information Security Program
2. IT0120 - Secure Network Infrastructure
3. NIST Glossary of Terms