THE UNIVERSITY OF TENNESSEE
HEALTH SCIENCE CENTER

UT Health Science Center: AC-001.04-VPN Access	
Version 2	**Effective Date: 09/30/2017**

Responsible Office: Office of Cybersecurity	Last Review: 03/23/2020 Next Review: 03/23/2022
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

The purpose of this Practice is to provide access via Virtual Private Network (VPN) connections to the UTHSC network from remote hosts, untrusted hosts, and remote networks via VPN to minimize the potential exposure from unauthorized access to UTHSC resources.

Scope

This practice applies to all remote access via VPN connections to the UTHSC network from remote and/or untrusted devices and networks.

Practice

1. Only approved UTHSC faculty/staff and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs.
2. VPN is a "user managed" service, meaning that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.
3. VPN Access is granted on an “as needed” basis. Access may be granted to groups of users when a need is well documented. All other persons must to apply for VPN access using the VPN Access Request Form (https://uthsc.edu/vpn/index.php)
4. Users with VPN privileges must ensure that unauthorized users are not allowed access to UTHSC internal networks via the user’s VPN.
5. Dual tunneling (also called split tunneling) is NOT permitted; only one network connection is allowed. All traffic during the VPN connection will go through the UTHSC network and will be subject to the same controls as Intranet traffic.
6. VPN Concentrators/Gateways are installed and managed by the UTHSC ITS.
7. For workstations (desktops and laptops), only the ITS approved VPN client may be used.

8. Any device and/or network connected via VPN 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 via VPN or any other technology must use up-to-date anti-virus software.
    b. All computers connected to UTHSC internal networks via VPN must have the latest operating system security patches applied.
    c. VPN use is controlled minimally using password management and two-factor authentication.
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. Standard-ITS-GP-004-Definitions
2. Standard-InfoSec-AC-001-Access Controls
3. Standard-InfoSec-AC-002-Authentication
4. Practice-InfoSec-AC-002.02-Password Management and Complexity