HSCEP OP: 56.10.05, **Network Access**

PURPOSE: To define network access.

REVIEW: Policy will be reviewed once a year by the Director of Network Operations and will be approved by the Chief Information Officer (CIO) every odd-numbered year.

POLICY/PROCEDURE:

Local Area Networks

Supported LANs are those designed, installed, and operated by the Network Operations team. Devices such as computers, zero clients, phones, printers, scanners, storage devices, Internet of Things (IOT) and videoconferencing systems may be connected to a network outlet within a supported LAN with the approval of the Director of Network Operations.

The following may not be connected to an outlet within the TTUHSC El Paso network without prior written authorization of the Director of Network Operations or his/her designee:

- Proxy servers and firewalls
- Systems or devices providing virtual private networking (VPN) capability to the internet
- Wireless devices, rogue access points or peers and hot spots
- Network devices
- Systems or devices containing a network adapter operating in promiscuous mode where a node on a network accepts all packets, regardless of their destination address
- Network Sniffers
- Systems performing network address translation (NAT)
- Systems operating a domain naming system (DNS), Windows internet naming system (WINS), or dynamic host configuration protocol (DHCP) services
- Windows domain controllers

TTUHSC Domain

All TTUHSC El Paso-owned PCs and servers attached to the TTUHSC El Paso network must be members of the TTUHSC domain and defined in the appropriate active directory organization unit (OU)

Remote Access Policies and Procedures

Remote access to the TTUHSC El Paso network provides users with the convenience of accessing the internet, their office computer, or information on network file shares to which they have access. Along with this convenience comes the need for appropriate security controls to ensure that data transmitted is secure.

Additionally, the network must be protected from illicit use to ensure that viruses, malware, and other malicious code are not allowed to propagate across the network.

Scope

This policy applies to all hard wired, wireless and remote devices connected to the TTUHSC El Paso network infrastructure through network access.

Policy

State and federal legislation requires TTUHSC El Paso to provide protection of sensitive data such as patient information and student financial data. Therefore, TTUHSC El Paso personnel must use a secure mechanism for accessing the TTUHSC El Paso network infrastructure remotely. Additional information on remote access can be found under the IT access control policy at www.ttuhscep.edu/it/policies.

All users who connect to the TTUHSC El Paso network must have an up-to-date anti-virus software installed on all devices. This anti-virus software must be updated regularly with new anti-virus signatures. ~~TTUHSC El Paso provides free McAfee Virus Scan licenses? *Please validate, according to the link below there is a charge associated with it* for home use by faculty, staff, and students. This software can be downloaded at https://ttuhscep.edu/it/IT-store/software.aspx.~~

Formatted: Font: Italic, Underline

VPN

Any user accessing the TTUHSC El Paso network through an internet connection (satellite or cable) must connect using a virtual private network (VPN) connection, except for Virtual Desktop Infrastructure (VDI) access.

Client Connection Setup

VPN services from connections outside the TTUHSC El Paso network are supported for eRaider accounts, providing services are in compliance with the internet service provider (ISP)'s policies.

Security

All institutional cybersecurity policies are applicable to network access users. Cybersecurity controls in place include appropriate authentication and intrusion prevention services (IPS). Monitoring and auditing will be conducted for network access connections. In the event of unusual, disruptive, or suspicious network activity, Information Technology will disable the eraider account, based on recommendations from the TTUHSC El Paso IT Cybersecurity team.

TTUHSC El Paso Software Requirements

All systems connected to the TTUHSC El Paso network must have approved anti-virus software installed and operational before the system may be connected to the network. This software must be configured to receive regular virus signature updates from the anti-virus servers administered by the TTUHSC El Paso information cybersecurity officer and his/her staff.

Disclaimer Statement. TTUHSC El Paso reserves the right to interpret, change, modify, amend or rescind any policy in whole or in part at any time without the consent of employees.