Chapter 5	Information Management & Services	Effective:	June 2002
Section 5.8	Information Security	Revised:	October 2015
Policy 5.8.7	**Network Access Policy**	Responsibility:	Chief Information Security Officer

NETWORK ACCESS POLICY

Overview

This document establishes the policy for access to and from the Health Science Center computer network. This policy is designed to encourage efficient use of the computer network while minimizing the potential exposure to damage that may result from unauthorized use.

Policy

1. Network routers, switches, wireless access points and hubs are points of vulnerability and need to be managed centrally to ensure integrity, security, reliability, and availability. Computer network users may not use one of these or other devices to extend or re-transmit network services without the approval of Systems and Network Operations (SNO). Only one device (computer, printer, etc) may be connected to a computer network outlet, with the single exception being institutional computers connected through University-issued Voice-Over-IP phones. The use of multiple network interface cards ("dual-homed" or "multi-homed") in a single computer to facilitate multi-Virtual Local Area Network (VLAN) access creates a bypass of VLAN security and is prohibited.

2. Non-standard devices (other than desktop or laptop computers) must be approved by SNO before being connected to the computer network at any campus location or other extended computer network location.

3. Access to the wireless computer network is provided through installation of the University's security certificate and usage of University-issued credentials. Wireless access is limited to mobile devices only (laptops, tablet computers, smartphones, etc.).

   The wireless computer network is a shared access technology, meaning all the portable computers in a coverage area are sharing the available bandwidth; for this reason, wireless printers and desktop computers with wireless cards are prohibited. Also, the use of any technology with interferes with the normal operation of the wireless network is prohibited. This technology includes, but is not limited to:

- wireless systems configured in “ad hoc” mode instead of “infrastructure” mode,

- systems which bridge the wireless and cellular networks (also known as “personal hotspots or MiFi”),

- and the introduction of unsanctioned wireless access points (also known as “rogue APs”)

Should these or any other technologies affect the availability of the wireless network or represent a threat to University users, they will be disabled without notice, and in extreme cases may be confiscated.

Should the wireless capacity in an area be over-utilized on a routine basis, SNO may require some portable computers to connect to the wired network.

4. Access to the computer network from the Internet is important for ease of use, but is frequently used by intruders for destructive intrusion. All remote access to the protected side of the computer network will be through secure means, such as a virtual private network (VPN). Additional authentication may be required.

   Direct connections via common carrier circuit are limited to circuits installed and maintained by SNO. The use of modems or modem pools on the computer network is restricted to those ensuring security and approved by SNO and Information Security.

5. Standard applications, such as Web, Telnet and File Transfer Protocol (FTP) requiring access to the Internet are allowed within reason.

   - Other applications, such as peer-to-peer file sharing can enable the Health Science Center computer network to act as an agent to cause harm to other computer networks or use excessive bandwidth that impairs priority traffic; for this reason, peer-to-peer file sharing is prohibited.

- SNO may block, restrict or limit application traffic as needed to ensure adequate bandwidth for priority applications and ensure use of resources is for Health Science Center business.

- Network users cannot make network usage decisions on behalf of the University; this capability is exclusively the function of SNO. Those usage decisions include the installation of any operating system or application that can re-utilize network for non-University purposes.

6. The Health Science Center computer network firewall plays a major role in information security. It is important that this appliance restrict access to the protected side of the network as much as possible. Publicly accessible services, including Web access and FTP are provided outside the firewall from the demilitarized zone (DMZ) only, or through network management devices maintained and operated by SNO. The DMZ must be a physical or logical DMZ maintained by SNO. Exceptions must ensure security and obtain approval via a waiver authorized by SNO and Information Security.

   Only SNO managed internal firewalls will be allowed to securely connect subnets (VLANs) within the computer network. The use of host-based firewall products is encouraged to protect individual systems.

7. Unauthorized deliberate attempts to obtain unpublished computer network information are prohibited by University policy and by State and Federal law. This prohibition applies to all campus computer network locations, and the wide area network, and includes practices such as “packet sniffing,” “password cracking,” and “port scanning” both wired and wireless.

8. Any attempt to disrupt service or performance of computer systems at any campus location is prohibited and can result in the loss of computer network privileges and disciplinary action. This includes any form of action that denies service through programmatic operation of a network device or through physical means, that attempts to gain unauthorized access to data, or that attempts to elevate user privileges beyond appropriate levels.

9. Computer network users are permitted to use only those network (IP) addresses issued by SNO. Selecting an IP address at random to configure a computer network device is prohibited; specific static addresses may be requested from SNO. The use of private IP addressing behind firewalls and proxy servers, as well as the use of network address translation (NAT) is prohibited without authorization from SNO.

10. Network operational applications such as directory service (DNS, WINS, etc.) or network address space services (DHCP) need to be provided centrally to ensure manageability and reliability. Providing these services independently is prohibited without authorization from SNO.

Accountability

Departmental

Deans, Chairs, and Directors are accountable for ensuring that their department remains in compliance with all applicable local, state, and federal information security policies as described in Section 4.9.2 of the *Handbook of Operating Procedures* (HOP), "Management's Responsibilities". If it is determined that the University's network, systems, data, or mission have been placed at risk due to a willful or negligent lack of compliance with information security policies, Information Management and Services (IMS) personnel are authorized to terminate service as appropriate to mitigate the risk. Additionally, IMS is authorized to assess the department a service fee for security remediation and/or reconnection of services. The service fee will be charged to the department's state funds account.

Individual

Violations of this policy are subject to disciplinary action as described in Section 2.1.2, "*Handbook of Operating Procedures",* of the HOP.