

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	September 2004
Policy 5.8.8	Computer Network Security Configuration	Responsibility:	Vice President and Chief Information Officer

COMPUTER NETWORK SECURITY CONFIGURATION

Policy

The purpose of the Health Science Center's "Computer Network Security Configuration" policy is to establish the rules for the maintenance, expansion and use of the computer network infrastructure. These rules are necessary to preserve the integrity, availability of services and confidentiality of Health Science Center information.

- Systems and Network Operations (SNO) is responsible for the computer network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
- To provide a consistent computer network infrastructure capable of exploiting new networking developments, all cabling must be installed by SNO or an approved contractor.
- All equipment connected to the computer network must be configured to a specification approved by SNO.
- All hardware connected to the computer network is subject to SNO and/or Information Security Office (ISO) monitoring standards. SNO reserves the right to remove any device that does not comply with standards or is not considered to be adequately secure.
- Changes to the configuration of active computer network management devices must not be made without the approval of SNO.
- The computer network infrastructure supports a well-defined set of approved networking protocols. Any use of non-sanctioned protocols must be approved by SNO.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by SNO.
- All connections of the network infrastructure to external third party networks are the responsibility of SNO. This includes connections to external telephone networks.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	September 2004
Policy 5.8.8	Computer Network Security Configuration	Responsibility:	Vice President and Chief Information Officer

-
- All firewalls must be installed and maintained by SNO unless written authorization is obtain from SNO and the Chief Information Security Officer (CISO).

 - No extension or retransmission of computer network services by installation of a router, switch, hub, wireless hub or dual ported computer is permitted.

 - No computer network hardware or software that provides network services can be installed without SNO approval.

 - Computer network hardware can only be modified by the staff of SNO.
-