

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.13	Security Monitoring	Responsibility:	Chief Information Security Officer

SECURITY MONITORING

Policy

The Information Security Function (ISF) is authorized and responsible for the implementation and execution of this policy. Towards this end, the ISF has the authority to:

1. Use automated tools to provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed and the tools will report exceptions. These tools will be deployed to monitor:
 - a. Internet traffic
 - b. Electronic mail traffic
 - c. LAN traffic, protocols, and device inventory
 - d. Operating system security parameters
2. Check following files for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
 - a. Automated intrusion detection system logs [Systems and Network Operations (SNO), Information Security]
 - b. Firewall logs [SNO; Information Security]
 - c. User account logs [Accounts Management]
 - d. Network scanning logs [SNO; Information Security]
 - e. System error logs [Assigned System Administrator]
 - f. Application logs [Assigned System Administrator]
 - g. Data back-up and recovery logs [Assigned System Administrator]
 - h. Help desk trouble tickets [[IMS Service Desk](#)]

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.13	Security Monitoring	Responsibility:	Chief Information Security Officer

-
- i. Telephone activity – Call detail reports [SNO]
 - j. Network printer and fax logs [Assigned Administrator]
3. Perform the following checks on a periodic basis by:
- a. Password strength
 - b. Unauthorized network devices
 - c. Unauthorized personal web servers
 - d. Unsecured sharing of devices
 - e. Unauthorized modem use
 - f. Operating system and vulnerabilities
 - g. Software licenses
4. Report any security issues discovered to the Chief Information Security Officer (CISO) for follow-up investigation.
5. Provide investigative security monitoring as requested by law enforcement entities. Personnel authorized to conduct information security monitoring in support of investigations, must be designated in writing.

Security monitoring, penetration tests, and investigation assistance is limited to those designated by the Information Resources Manager (IRM). Any monitoring conducted on the University network will be guided by the processes and procedures developed by the Department of Information Security and Assurance. This includes but not limited to, designating predetermined scanning windows, scripted penetration tests, and an approved tools list.
