Chapter 5	Information Management & Services	Effective:	June 2003
Section 5.8	Information Security	Revised:	October 2016
Policy 5.8.13	**Security Monitoring**	Responsibility:	Chief Information Security Officer

SECURITY MONITORING

Policy

Security monitoring of network, operating system and application platform activity is the exclusive responsibility of the Chief Information Security Officer. Responsibility to perform monitoring activities as defined in policies, standards and procedures may be assigned to an employee or third-party/vendor by the Chief Information Security Officer and documented in an associated job description or contract.

The Chief Information Security Officer shall adopt and document policies, standards and procedures to ensure:

1. Network traffic and use of Information Resources (including, but not limited to, all internal and business partner networks, Internet, electronic communication, wide area and telecommunication networks and protocols and operating system and application parameters) is monitored as authorized by federal and state laws and regulations and only for purposes of fulfilling UT Health San Antonio's mission and securing its operations;

2. Server, application and network logs (including, but not limited to, back up logs, telecommunication activity reports, software licensing reports and incident/service request tickets) are reviewed manually or through automated processes on a scheduled basis based on risk, remediation procedures and regulation to ensure that Information Resources containing Confidential/High Risk data are not being appropriately accessed;

3. Vulnerability assessments are performed annually, at minimum, to identify software and configuration weaknesses within information systems maintained in both Centralized and Decentralized IT;

4. Assess and restrict access of unauthorized Information Resources and applications (including, but not limited to, web servers; application, file and storage servers; wireless access points; unauthorized and unlicensed software; and network devices).

5. An annual external network penetration test is performed by an independent third-party; and

6. That results of log reviews, vulnerability assessments, penetration tests, and IT audits are available to the Chief Information Security Officer and that required remediation is implemented.

All monitoring not defined in UT Health San Antonio policy and/or explicitly permitted by the Chief Information Security Officer is deemed a Security Incident and actions to restrict and mitigate such activity shall be performed.

Reference

- U.T. System Policy 165 Standard 17