| | | | |
|---|---|---|---|
| Chapter 5 | Information Management & Services | Effective: | June 2003 |
| Section 5.8 | Information Security | Revised: | June 2018 |
| **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.

The Chief Information Security Officer must ensure:

1. that 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, protocols and services) is monitored as authorized by federal and state laws and only for purposes of fulfilling UT Health San Antonio's mission and securing its data, systems and employees;

2. server, application and network logs 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 inappropriately 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. an annual external network penetration test is performed; and

5. 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 considered unauthorized and manual or automated actions to restrict and mitigate such activity or connectivity shall be performed.

Responsibility to execute 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.

## Reference

- U.T. System Policy 165 Standard 17