5.8.13 Security Monitoring

Chapter 5 - Information Technology	Original Effective Date: June 2003
Section: 5.8 Information Security	Date Last Reviewed: February 2023
Responsible Entity: Chief Information Security Officer	Date Last Revised: June 2018

I. Purpose

To establish the standard for security monitoring of network, operating systems, and application platforms.

II. Scope

This policy applies to all current and former faculty, staff, students, residents, healthcare providers, researchers, contractors, or any other third-party entities who have direct or indirect access to Information Resources created, held or maintained by UT Health San Antonio or any controlled affiliate, including, but not limited to its clinics, hospitals, and research operations.

III. Policy

A. Security monitoring of network, operating system and application platform activity is the exclusive responsibility of the Chief Information Security Officer.

B. 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.

C. 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.

D. 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.

IV. Definitions

There are no defined terms used in this Policy.

V. Related References

There are no related documents associated with this Policy.

VI. Review and Approval History

A. The approving authority of this policy is the University Executive Committee.

B. The review frequency cycle is set for three years following the last review date, a time period that is not mandated by regulatory, accreditation, or other authority.

Effective Date	Action Taken	Approved By	Date Approved
06/2003	Policy Origination		
06/2018	Policy Revision		
02/2023	Policy Review/Discretionary Edits		