Policy Summary: The operating system or environment for all information system resources must undergo a regular vulnerability assessment.

Purpose: This policy reflects our commitment to identify and implement security controls which will keep risks to information system resources at reasonable and appropriate levels.

Policy: Vulnerabilities to the operating system or environment for information system resources must be identified and corrected to minimize the risks associated with them.

To ensure these vulnerabilities are adequately addressed, the operating system or environment for all information system resources must undergo a regular vulnerability assessment.

The frequency of these vulnerability assessments will be dependent on the operating system or environment, the information system resource classification, and the data classification of the data associated with the information system resource. See Information System Vulnerability Testing Standard.

Documentation: All data collected and/or used as part of the Risk Management Process and related procedures will be formally documented and securely maintained.

Scope/Applicability: This policy is applicable to all departments that operate information systems.

Regulatory Reference: HIPAA 45 CFR 164.308(a)(1)(ii)(B)
Payment Card Industry Data Security Standard

Definitions: See the Information Security Policy Definitions document for definitions

Responsible Department: Each organizational unit which manages its own information systems is responsible for complying with this policy.

Enforcement/Audit: The university’s Internal Auditing department is responsible for monitoring and enforcement of this policy.

Related Policies: Information System Vulnerability Testing Standard, Risk Analysis, Data Classification, Resource Identification, Resource Classification

Procedures: Contact the OUHSC IT Service Desk

Renewal/Review: This policy is to be reviewed and updated as needed by IT Information Security Services.