UNIVERSITY OF OKLAHOMA
Information Technology
Security Policies

Subject: Information System Workstation Use and Security Policy	**Coverage:** OUHSC
Policy #: Information Security-P# 9.2.1	**Version:** 2.0
Regulation: HIPAA, GLB, State of Oklahoma	**Approved:** 03/14/07
Effective: 03/14/07	**Revised/Reviewed:** 11/21/2014

Policy Summary:

Procedures must be in place to ensure all University workstations are classified based on allowable capabilities and activities and secured accordingly.

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:

Procedures must be in place to ensure all University workstations are classified based on allowable capabilities and activities and secured accordingly in order to protect the confidentiality, integrity, and availability of *sensitive* data contained on or accessed through the workstations.

This includes defining the functions to be performed, the manner in which they are to be performed, and the physical attributes of the surroundings of a specific workstation or group/class of workstations which contain or provide access to *sensitive* data.

The level of protection provided for University workstations containing or providing access to *sensitive* data must be commensurate with the identified risks. An assessment of the risks to University workstations which contain or provide access to *sensitive* data, including a vulnerability scan and corrective actions per the Vulnerability Assessment Standard.
The risk assessment documentation must be securely maintained.

At a minimum the following controls must be in place for University workstation containing or providing access to *sensitive* data:

- Must require a form of unique user authentication such as: user ID and password, biometrics, or an access device such as a token for authentication of access.

- Must be part of a patch or vulnerability management system.

- Must be physically located in such a manner to minimize the risk of unauthorized access.

- Display screens/monitors must be positioned such that information cannot be readily viewed by unauthorized individuals.

University Faculty, staff, students, and volunteers must report loss or theft of any access device (such as a card or token) that allows them physical access to areas having workstations which contain or provide access to sensitive data.

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 OUHSC.

Regulatory Reference:	HIPAA 45 CFR 164.308(a)(1)(ii)(B) 16 CFR Part 314 Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act (‘‘G–L–B Act’’) State of Oklahoma Information Security, Policy Procedures Guidelines 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:	Risk Analysis, Data Classification, Resource Identification, Resource Classification
Renewal/Review:	This policy is to be reviewed and updated as needed by IT Information Security Services.