

UNIVERSITY OF OKLAHOMA
Information Technology
Security Policies

Subject: Information System Facility Security Policy
Policy #: Information Security-P#9.1
Regulation: HIPAA, GLB, State of Oklahoma
Effective: 04/11/07

Coverage: OUHSC
Version: 2.0
Approved: 04/11/07
Revised/Reviewed: 11/14/2014

Policy Summary:	<p>The University must establish procedures to protect Sensitive Information System Resources and Data from unauthorized physical access, tampering, and theft.</p>
Purpose:	<p>This policy reflects the University's commitment to identify and implement security controls that will keep risks to Information System Resources at reasonable and appropriate levels.</p>
Policy:	<p>The University must protect the confidentiality, integrity, and availability of its Information Systems by preventing unauthorized physical access to, tampering with, and theft of these systems and the facilities in which they are located, while ensuring properly authorized access is allowed.</p> <p>Information System Resources containing Sensitive Data must be physically located in areas where unauthorized access is minimized. The perimeter of a building or site containing Information Systems with Sensitive Data must be physically sound, the external walls of the site should be solidly constructed and all external doors must have appropriate protections against unauthorized access.</p> <p>The level of protection provided for Information System Resources containing Sensitive Data must be commensurate with identified risks and aligned with Information System resource classification. An annual assessment of risks to the facilities storing Information Systems with Sensitive Data must be performed by Resource Owners or Resource Owner Representatives.</p> <p>An annual inventory of all physical access controls used to protect Information Systems resources with Sensitive Data and hosting facilities must be performed. All repairs and modifications to the physical components of hosting facilities that are related to security must be documented. This documentation must be stored in a secure manner.</p> <p>All physical access rights to areas where Information Systems Resources containing Sensitive Data are maintained must be clearly defined and documented. Such rights must be provided only to University Workforce Members having a need for specific access in order to accomplish the responsibilities of their positions and must be regularly reviewed and revised as necessary.</p> <p>All Workforce Members must wear the organization's employee identification visibly. Employees should be encouraged to report unescorted strangers or anyone not wearing visible identification. All visitors with a requirement for access to the facility must show proper identification and sign in prior to gaining physical access to areas where Information System resources containing Sensitive Data are located.</p> <p>The University must maintain, regularly review and revise a formal, documented facility security plan in accordance with the Facility Security Plan Standard.</p>

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 Workforce Members.
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
Definitions:	See the Information Security Policy Definitions document for definitions
Responsible Department:	Each business unit within the OUHSC and the Health Care Components that 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 and Classification
Renewal/Review:	This policy is to be reviewed and updated as needed by IT Information Security Services.