UNIVERSITY OF OKLAHOMA
Information Technology
Security Policies

Subject: Information System Development Security Policy	**Coverage:** OUHSC
Policy #: Information Security-P#12.0	**Version:** 2.0
Regulation: HIPAA, GLB, State of Oklahoma	**Approved:** 05/09/07
Effective: 05/09/07	**Revised/Reviewed:** 11/20/2014

Policy Summary:	All information system resources which store, receive or transmit sensitive data must have security reviews conducted throughout its system development life cycle (SDLC).
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:	Security reviews must be conducted throughout each phase of the System Development Life Cycle (SDLC) for information system resources which receive, store, or transmit sensitive data. Security reviews are necessary to keep risks at reasonable and appropriate levels. The following defines the minimum review requirements for each phase: • Feasibility Phase – high level review to ensure security requirements can support the business case • Requirements Phase – define any initial security requirements or controls to support the business requirements • Design Phase – verify appropriate security controls for the baseline have been identified and ensure change control is established and used for the remainder of the SDLC. Repeat verification with each design change or as warranted • Development Phase – to verify and validate all security controls identified from design phase. Repeated throughout as changes are made or as warranted • Implementation Phase – final verification of existing controls and the appropriate levels of risk mitigation These security reviews must be documented as part of the complete record of the SDLC for this resource.
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) 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 (PCI DSS)
Definitions:	See the Information Security Policy Definitions document for definitions
Responsible Department:	Each organizational unit within the University of Oklahoma 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, Resource Classification

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