UNIVERSITY OF OKLAHOMA
Health Sciences Center
Information Technology
Security Policy

Information System Product Review

Purpose:	The purpose of this policy is to establish requirements for reviewing Information Systems (IS) to identify risks and recommend appropriate security controls to mitigate identified risks to an acceptable and reasonable level. IS will also be reviewed to determine if it is compatible with existing University technology infrastructure.
Policy:	Business Units must request a Product Review from Campus IT for all IS receiving, storing, processing, and/or transmitting University data. During the Product Review the Business Unit must provide, at a minimum, a complete description of the product, its functions and capabilities, interfaces with other systems and data, the method of interface, and all inputs and outputs. If any of the above descriptions change at any time the Product Review request must be updated to reflect these changes and be resubmitted to Campus IT. The following requirements must be met as part of the As part of the Product Review process: 1. All data and IS, Cloud Service Providers, and third-party web development efforts must have roles assigned by the Business Unit in accordance with the Information Security Roles and Responsibilities Policy. 2. All data and IS, Cloud Service Providers, and third-party web development efforts must be classified in accordance with the IS and Data Classification Policy. 3. All new data and IS, Cloud Service Providers, and third-party web development efforts classified as Category A or B will undergo a solution architecture review by Campus IT. 4. All IS and data, Cloud Service Providers, and third-party web development efforts classified as Category A must have undergone an initial and will undergo an annual, thorough assessment of security controls. 5. All IS and data, Cloud Service Providers, and third-party web development efforts, classified as Category B must undergo an assessment of security controls via the Product Review or Vendor Review questionnaires every three (3) years. 6. Campus IT's risk recommendation actions in response to the Product Review must be addressed in a timely manner, as evidenced by documentation supplied to Information Security. In addition to a Product Review, appropriate business agreements and approvals are required. The requesting department retains responsibility for ensuring this product is compliant with all applicable policies and regulations.
Scope/Applicability:	This policy is applicable to the OU Health Sciences Center and OU Health Care Components.

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 (‘‘GLB Act’’) • FERPA: 34 CFR Part 99 [Family Educational Rights and Privacy Act] • Payment Card Industry Data Security Standard • State of Oklahoma Information Security, Policy Procedures Guidelines
Definitions:	Information Technology Policy Definitions **Business Unit:** As applied to the University, a Business Unit may be a department, a program or college, a support service or central administration function within the University. A business unit may extend across multiple locations. **Information System (IS)**: A system and/or service, which typically include: hardware, software, data, applications and communications that support an operational role or accomplish a specific objective. *Note – An IS can reside on premise or off-premise. **IS Sponsor:** an individual responsible for providing the necessary funding and support for the IS Owner and Administrator to perform their roles and responsibilities. The IS Sponsor provides executive oversight of data and/or IS and assumes responsibility for policy compliance for the IS under his or her control. The IS Sponsor reviews high level risk items of the IS and makes risk treatment decisions for the Business Unit. **IS Owner:** the individual responsible for maintaining a current inventory of all ISs within the business unit, classifying the data and IS, establishing rules for disclosing and authorizing access to IS data, conducting access control reviews, coordinating with campus IT to conduct risk assessments and serving as the escalation contact for the IS Administrator. **IS Owner Representative*:*** An individual designated by the IS Owner to act on his or her behalf. **IS Administrator:** An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an information technology device or system (e.g., system administrator or network administrator). At OUHSC the IS administrator role is typically performed by the business unit Tier One. The IS administrator role may be performed through an agreement between the business unit and Campus IT. For additional Information Technology definitions, see Information Technology Policy Definitions Document at http://it.ouhsc.edu/policies/documents/infosecurity/Information%20Security%20Policy%20Definitions.pdf
Responsible Department:	Any entity within the University of Oklahoma managing an IS that views, stores, transmits, and/or collects University data is responsible for complying with this policy.
Policy Authority/ Enforcement:	This policy is authorized and approved by the OUHSC Dean’s Council and the Senior Vice President and Provost. Internal Audit may periodically assess Business Unit compliance with this policy and may report violations to the Board of Regents.

Table 1 Revision History

Revision Date	Version	Revised By	Changes Made
03/21/2006	1.0	Campus IT	Baseline Version
12/19/2014	2.0	Campus IT	Modified purpose of policy statement Expanded the scope to include all Products, not just "sensitive". Added new policy process statements. Simplified naming scheme of "Information System Resource" to remove the word "Resource"
01/15/2015	2.1	OUHSC Information Security Review Board (ISRB)	Revised last paragraph in the policy about the Product Review not implying consent to purchase since it was confusing. Added that "appropriate business agreements and approvals need to be in place".

Table 2 Approval History

Version	Approval Date	Approved by:	Title:
1.0	07/11/2006	Dean's Council and Senior Vice President Provost	
2.1	01/15/2015	Dean's Council	

Table 3 Review History

Version	Review Date	Reviewed by:	Title:
1.0	01/31/2007	OUHSC Policy Communication and Coordination Committee	
2.1	01/15/2015	ISRB	See ISRB membership list