UNIVERSITY OF OKLAHOMA
Health Sciences Center
Information Technology
Security Policy

Business Unit Information Security Roles and Responsibilities

Purpose:

It is essential that University Business Units be aware of information security risks and their roles and responsibilities for mitigating these risks. Information security incidents can have significant business impacts on, as well as implications for, the University's compliance with federal and state regulations and the terms of certain grants and contracts.

This policy reflects the University's commitment to identify and implement security controls that mitigate Information Systems (IS) risks to reasonable and acceptable levels. IS are assets of the University and require the assignment of the security responsibilities below to the appropriate individuals or departments.

Policy:

Deans and administrative heads who oversee University of Oklahoma Health Sciences Center Business Units that manage their own IS must designate in writing the employees (by name or position/title) who will fulfill each of the defined roles and responsibilities of this policy:

1. **IS Sponsor,** who will be responsible for the following:
    a. Provide spending authority and support necessary for the IS Owner and Administrator to perform their roles and responsibilities.
    b. Oversee data and/or IS processes and procedures to ensure compliance with applicable policies and regulations.
    c. Review high level risk items of the IS and make risk management decisions for the Business Unit.
    d. Serve as the escalation point of contact for IS Owner responsibilities
2. **IS Owner,** who will be responsible for the following:
    a. Maintain and document a current inventory of all IS within the Business Unit.
    b. Classify the IS and data according to the IS and Data Classification policy and standard.
    c. Establish rules for disclosing information from and authorizing access to IS and data.
    d. Conduct yearly access control reviews in cooperation with Information Technology.
    e. Conduct yearly IS and classification reviews in cooperation with Information Technology.
    f. Ensure Information System Product Reviews are conducted with Campus IT for all new IS. See IT's Information System Product Review Policy.
    g. Coordinate with Information Security to conduct an annual risk assessment for IS classified as Category A.
    h. Serve as the escalation point of contact for IS Administrator duties.
3. **IS Administrator,** who will be responsible for the following:
    a. Ensure all IS software is current and supported.
    b. Sign-up to receive security and software update notices from software vendors for software that is part of the IS.
    c. Deploy and document vulnerability management procedures and provide a copy to OUHSC Information Security. See IT's Vulnerability Assessment policy and standard.

d. Deploy and document patch management procedures and provide a copy to OUHSC Information Security.
e. Deploy and document audit and accountability procedures and provide a copy to OUHSC Information Security. See IT's IS Activity Review policy.

Campus IT Roles and Responsibilities:

In order to assist the Business Units in accomplishing the objective of mitigating risks to reasonable and acceptable levels, Campus IT employees have defined roles and assigned responsibilities that may include, but are not limited to:

a. Assist IS Owner in conducting Product Reviews.
b. Receive and address requests for exceptions to security roles and responsibilities.
c. Maintain a current list of exceptions to security roles and responsibilities.
d. Review annually all exceptions to security roles and responsibilities.
e. Maintain overview responsibility for implementation of this policy.
f. Train and educate the University community on this policy.
g. Monitor technological developments and changes in the law, user behavior, and the market, and update this policy in response, as appropriate.
h. Receive and maintain an inventory of all IS holding University confidential (Category A) information.
i. Assist IS Owner in conducting risk assessments of all IS classified as Category A.

Scope:

This policy is applicable to all OUHSC Business Units that operate IS.

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]
- State of Oklahoma Information Security, Policy Procedures Guidelines
- Payment Card Industry (PCI) Data Security Standard v3.0

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 that typically includes 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 IS 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 IS (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 Health Sciences Center managing an IS that processes, 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
11/14/2014	1.0	Campus IT	Baseline Version
01/06/2015	1.1	Campus IT	Modified Purpose statement per IT leadership suggestions and added definition for Business Unit and modified definitions for Business Unit Executive Sponsor and IS Owner.
01/15/2015	1.2	OUHSC Board (ISRB)	Added " and administrative heads" to first policy sentence. Revised "IS Owner f." sentence to indicate a Product Review is required (the Product Review will include a solution architecture review.)
10/09/2015	1.3	OUHSC ISRB	Added "in writing the" and "(by name or position/title)" to first sentence of policy statement.

Table 2 Approval History

Version	Approval Date	Approved by:	Title:
1.2	01/15/2015	OUHSC Dean's Council	
1.3	11/11/2015	OUHSC Dean's Council	

Table 3 Review History

Version	Review Date	Reviewed by:	Title:
1.2	01/15/2015	ISRB	See ISRB membership list
1.3	10/13/2015	ISRB	