

Business Unit Information Security Roles and Responsibilities

Current Version	Compliance Date	Approved Date
2.3	12/31/2017	03/06/2018

1. Purpose

It is essential that University faculty, residents, fellows, staff, students, volunteers, and third party suppliers be aware of information security risks and their roles and responsibilities for mitigating these risks. Information security incidents can have significant business impacts on the University, 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.

2. 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.

For additional Information Technology definitions, see Information Technology Policy Definitions Document at <http://it.ouhsc.edu/policies/documents/infosecurity/Information%20Security%20Policy%20Definitions.pdf>.

3. Policy

Business Units that manage their own IS must designate the employees (by name or position/title) who will fulfill each of the defined roles and responsibilities of this policy during the OUHSC Information Security Risk Assessment Process:

1. **IS Sponsor**, who is responsible for the following:
 - a. Review high-level information security risk items of the IS and make risk management decisions for the Business Unit, on behalf of the University.
 - b. Serve as the escalation point of contact for IS Owner responsibilities
2. **IS Owner**, who is 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 *OUHSC Information System and Data Classification Policy*.
 - c. Establish written rules for disclosing information from and authorizing access to IS and data, in accordance with the Information Security *OUHSC Access to University Data Policy*.
 - d. Conduct access control reviews of the IS in accordance with the Information Security *OUHSC Access to University Data Policy*.
 - e. Ensure Information Security Risk Assessments are conducted with OUHSC IT for all new IS, in accordance with the *OUHSC Information Security Risk Assessment Policy*.

- f. Ensure compliance with OUHSC Information Security policies and all regulatory requirements.
 - g. Serve as the escalation point of contact for IS Administrator duties.
- 3. IS Administrator**, typically a Tier 1 or other support personnel who is responsible for the management and support of technology assets within a Business Unit. IS Administrators must have recent and significant professional experience in computing or computing support and should have one of OUHSC's specific technology support job titles available from HR, who will be responsible for the following:
- a. Understand how IS and data are stored, processed, and/or transmitted.
 - b. Implement appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of IS, in accordance with the *OUHSC Information System and Data Classification Policy*.
 - c. Document and disseminate administrative and operational procedures to ensure consistent storage, processing, and transmission of IS.
 - d. Be responsible for the provision and de-provision of access to the IS, as authorized by the IS Owner.
 - e. Ensure proper participation with IT's *OUHSC Media Disposal Policy and Standard*.
 - f. Be responsible for all software acquisition, licensing and installation, configuration, and maintenance of the IS, as directed by the IS Sponsor and/or IS Owner.
 - g. Check for new operating system (OS) updates and install as they become available; this must be performed at least monthly.
 - h. Sign-up to receive security and software update notices from software vendors for software that is part of the IS supported or managed.
 - i. Coordinate an OUHSC Information Security Risk Assessment with OUHSC Information Security in accordance with the *OUHSC Information Security Risk Assessment Policy*.
 - j. Be responsible for setup and configuration of all wired and wireless connectivity for IS supported or managed.
 - k. Coordinate with OUHSC IT to ensure performance and integrity of campus IS.
 - l. Understand Information Security risks and how they impact the confidentiality, integrity, and availability of IS.

OUHSC IT Roles and Responsibilities:

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

- a. Assist IS Owner in conducting Information Security Risk Assessments.
- 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 among all Business Units.
- 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. As part of the Information Security Risk Assessment Process maintain an inventory of identified IS holding University Category A information.
- i. Assist IS Owners in conducting risk assessments of all IS classified as Category A.

4. Scope

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

5. Regulatory References

- State of Oklahoma Information Security Policies, Procedures and Guidelines Section 2.3 – Information Access
- State of Oklahoma Information Security Policies, Procedures and Guidelines Section 9.1 – Operating Procedures
- 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 (PCI) Data Security Standard v3.0

6. Authorization

This policy is authorized and approved by the OUHSC Dean’s Council and Senior Vice President and Provost and enforced by the IT Chief Information Officer. Internal Audit and other authorized departments of the University may periodically assess Business Unit compliance with this policy and may report violations to the University Administration and Board of Regents.

7. Policy Maintenance

This policy is scheduled to be reviewed, updated, and modified as necessary and at least annually.

8. Revision, Approval and Review

8.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	11/14/2015	OUHSC IT	Baseline Version
1.1	01/06/2015	OUHSC 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.
1.2	01/15/2015	OUHSC 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.)
1.3	10/09/2015	OUHSC ISRB	Added “in writing the” and “(by name or position/title)” to first sentence of policy statement.
2.0	11/14/2016	OUHSC IT	Applied new template. Updated enforcement statement.
2.1	08/25/2017	OUHSC IT	Updated policy references
2.2	12/4/2017	OUHSC IT	Updated IS Sponsor responsibilities. Updated IS Owner responsibilities. Updated IS Administrator responsibilities. Revised policy statement.
2.3	02/21/2018	OUHSC IT	Minor changes.

8.2 Approval History

Version	Date	Approved By
1.2	01/15/2015	OUHSC Dean's Council
1.3	11/11/2015	OUHSC Dean's Council
2.1	09/12/2017	Information Security Review Board
2.3	03/06/2018	Information Security Review Board

8.3 Review History

Date	Reviewed By
01/15/2015	OUHSC ISRB
10/13/2015	OUHSC ISRB
11/10/2016	OUHSC IT
10/28/2016	Legal Counsel
11/14/2016	OUHSC IT
08/25/2017	OUHSC IT
09/12/2017	OUHSC ISRB
12/1/2017	Information Technology Research Committee (ITRC)
02/19/2018	Legal Counsel