UNIVERSITY OF OKLAHOMA
Health Sciences Center
Information Technology
Security Policy

Information System and Data Classification Policy

Purpose: Information Systems and data are assets of the University. As assets they must be classified and protected according to the risks associated with their assigned classification. Certain classifications require additional levels of security controls to protect the confidentiality, integrity and availability of the system and data.

Policy: IS Owners must identify all IS and data within their Business Unit and follow these classification requirements:

1. Identify all IS and associated data
2. Classify all IS and data according to the Information System and Data Classification Standards below.
3. Maintain an inventory of the IS, data and its classification

The results of the classification will determine the level of security controls that must be applied to protect the IS, the physical location of the IS, and the frequency of assessment.

The examples below are not exhaustive; users should contact the appropriate office (Legal Counsel, Admissions and Records, Financial Services, etc.) for additional information.

	Category A **High Risk**	**Category B** **Medium Risk**	**Category C** **Low Risk**
Description	Data that is legally regulated and the associated IS to protect the confidentiality, integrity, and availability of the data, such as: • HIPAA • PCI • PII • FERPA Data or IS that would provide access to confidential information; Information System designated as "High Risk.	Data and associated IS, used in the conduct of University business, unless categorized as Category C or Category A; Data that the IS Owner and/or University executive leadership have determined not to publish or make public; Data protected by contractual obligations All public-facing IS (IS exposed to the Internet).	Data for which there is no expectation of privacy or confidentiality Data the University has made available or published for the explicit use of the general public.

Confidentiality	**Scope of access** Intended access by as few users as necessary and based on Minimum Necessary or Least Privilege principles. **Disclosure requirements:** May not be disclosed outside those allowed by role or need to know.	**Scope of access** Intended for access only by those with a need to know. **Disclosure requirements** Requires written permission of IS Owner to disclose.	**Scope of access** Intended for public Access. **Disclosure requirements** May be freely disclosed without permission.
Business Impact	Seriously impairs the functioning of the University or results in material financial, legal or reputational loss.	Significantly impairs the functioning of the University or results in significant financial, legal or reputational loss.	Negligible or no operational, financial, legal or reputational loss.
Examples *** exceptions apply**	**IS with access to Category A data** **Personally Identifiable Information (PII): Last name and first name or initial, with any one of the following:** • Social Security Number • Driver's license number • State ID card • Passport number • Financial account (checking, savings, brokerage, CD, etc.), credit card, or debit card numbers **Protected Health Information (PHI)** • Healthcare treatment or payment information • Health Plan	**IS of the following functions:** • Web servers • Database servers • E-mail servers • FTP Servers • Cloud Service Providers • Excel files containing confidential data • Access Databases containing confidential data **Personal/Employee Data** • Directory/contact information designated by the owner as private **Business/Financial Data** • Financial transactions that do not include confidential data • Information	**Certain directory/contact information not designated by the owner as private** • Name • Campus address • Email address • Listed telephone number(s) • Degrees, honors and awards • Most recent previous educational institution attended • Major field of study • Dates of current employment, position(s) • ID card photographs for University use **Specific for students:** • Class year • Participation in campus

	information **Personal/Employee Data** • OUHSC Employee ID Numbers • Income information and Payroll information • Personnel records, performance reviews, benefit information • Date and place of birth • Worker's compensation or disability claims **Student Data not included in directory information** • Loan or scholarship information • Payment history • Student tuition bills • Student financial services information • Class lists or enrollment information • Transcripts; grade reports • Notes on student performance • Disciplinary action • Athletics or department recruiting information **Business/Financial Data** • Credit card numbers with/without	covered by non-disclosure agreements • Contracts that don't contain PII • Credit reports • Records on spending, borrowing, net worth **Academic/Research Information** • Library transactions (e.g., circulation, acquisitions) • Unpublished research or research detail/results that are not confidential data • Private funding information • Human subject information • Course evaluations **Anonymous Donor Information** Last name, first name or initial (and/or name of organization if applicable) with any type of gift information (e.g., amount and purpose of commitment.) **Other Donor Information** Last name, first name or initial (and/or name of organization if applicable) with any of the following: • Telephone/fax numbers, e-mail & employment information • Family	activities and sports • Weight and height (athletics) • Dates of attendance • Status **Business Data** • Campus maps • Job postings List of publications (published research)

	expiration dates	information (spouse(s), partner, guardian, children, grandchildren, etc.) • Medical information **Management Data** • Detailed annual budget information • Conflict of Interest Disclosures • University's investment information **Information Technology Information** • Server Event Logs • Non-published Information Technology policy and procedures • Network diagrams Technical blueprints	

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

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 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
11/14/2005	1.0	OUHSC IT	Baseline Version
12/12/2014	2.0	OUHSC IT	Added new policy statements to reflect process requirements. Added clarification to the scope statement. Added classification table.
10/05/2015	2.1	OUHSC IT	Revised Purpose statement added "and data within their Business Unit" to the first sentence of the policy statement.

Table 2 Approval History

Version	Approval Date	Approved by:	Title:
1.0	11/16/2005	OUHSC Dean's Council and Senior Vice President and Provost	
2.0	01/26/2015	OUHSC Dean's Council and Senior Vice President and Provost	

Table 3 Review History

Version	Review Date	Reviewed by:	Title:
2.0	06/03/2016	OUHSC IT Information Security Services	Information Security Services

2.0	01/15/2015	ISRB	See ISRB membership list
2.0	10/05/2015	OUHSC IT Information Security Services	Information Security Services