Information System and Data Classification Policy

Current Version	Compliance Date	Approved Date
3.3	12/31/2017	12/12/2017

1. Purpose

Information Systems (IS) 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 of the system and data, in accordance with state and federal laws.

2. Policy

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

1. Inventory all IS and associated data, via an inventory list selected by the Business Unit.
2. Report the use of all IS and associated data to IT Security, via the *IS Risk Assessment Process.*
3. Coordinate the classification of all IS and data according to the Information System and Data Classification Standards below, with IT Security as part of the *IS Risk Assessment Process*.
4. Update the inventory of the IS, data, and data classification as needed and report any updates to IT Security.

The level of 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 Prohibited	Category B Restricted	Category C Confidential	Category D Public
Description	Data and associated IS that is legally regulated with a requirement to self-report to the government and/or provide notice to the individual if information is inappropriately accessed, such as: • HIPAA • PCI • PII • FERPA Information System designated as "High Risk."	Data and associated IS, used in the conduct of University business, in which the data is not legally regulated, but which an expectation of privacy or confidentiality exists; Data that the IS Owner and/or University executive leadership have determined not to publish or make public[1]; Data protected by contractual obligations; All public-facing IS (IS exposed to the Internet).	Data and associated IS not generally available to the public, and is not regulated or under contractual obligations for data protection.	Data that the University is under obligation to make available to the public. Data for which there is no expectation of privacy or confidentiality Data that the University or its employees have the right to make and have chosen to make available or to publish for the explicit use of the general public;
Common Classification Elements	• Social Security Numbers • Credit Card Numbers • Financial Account Numbers, such as checking or investment account numbers • Driver's License Numbers • Health Insurance Policy ID Numbers • Protected Health Information (ePHI) • Student Records • Export controlled information under U.S. laws • Human Participant Research Data	• Passport and visa numbers • Animal Research IACUC Protocol Data • Animal Research Veterinary Record Data • Admissions applications • Donor contact information and non-public gift amounts • Privileged attorney-client communications • Faculty/staff employment applications, personnel files, benefits information, salary	• Unpublished Research Data • Non-public OUHSC policies and procedure documentation • OUHSC internal memos and email, and non-public reports, budgets, plans, and financial information • Non-public contracts • University and employee ID numbers	• Information authorized on OUHSC websites without authentication • Published Research Data • Campus maps • Job postings • OUHSC directory contact information not designated by the individual as "private"
Shared Services Zone Placement	**S2 Business Zones - Required**	**S2 General Zones – Required**	**S2 General Zones - Recommended**	**N/A**

[1] Subject to applicable state or federal law

Risk Assessment Frequency	Every two (2) years	Every three (3) years	Every three (3) years	Every five (5) years
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 who have a need to know.	**Scope of Access** Intended for access only by those with a need to know. **Disclosure Requirements:** Requires written permission of IS Sponsor or contracting entity to disclose.	**Scope of Access** Intended for access only by those with a need to know. **Disclosure Requirements:** Requires written permission of IS Owner or contracting entity to disclose.	**Scope of Access** Intended for public Access. **Disclosure Requirements:** May be freely disclosed without permission, subject to other laws, such as patent and copyright laws.
Business Impact of Unauthorized Release	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.	Potential operational, financial, legal, or reputational loss.	Negligible or no operational, financial, legal, or reputational loss.

3. Roles and Responsibilities

IS Owner will be responsible for the following:

a. Providing details about any and all OUHSC IS and data to IT Security, to classify IS and data, according to this Information System and Data Classification Policy.

Information Security Services will be responsible for the following:

a. Reviewing, updating, and modifying the Information System and Data Classification Policy, annually and as needed if circumstances warrant.

4. Definitions

***Business Unit*:** As applied to the University, a Business Unit may be a department, a program or college, a support service, or a central administration function within the University. A Business Unit may extend across multiple locations.

Family Educational Rights and Privacy Act (FERPA): FERPA data is defined as a student's Personally Identifiable Information (PII), with any one of the following:

- Social Security number (or numbers derived from them)
- Course Grades
- Student Financial Numbers (Bursar's Office)
- Credit Card Numbers
- Wire Transfers
- Payment History
- Financial Aid/Grants
- Student Bills

- Driver's License
- State ID

Health Insurance Portability and Accountability Act (HIPAA): HIPAA data is defined as patient identifiable information, see *HIPAA Privacy Policy-01 Definitions.*

Information System (IS)*:* A system and/or service, typically including: 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 and may be owned or leased by the University.

IS Sponsor: An individual responsible for providing the necessary funding and support for the IS Owner and IS 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 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 also may be performed by OUHSC IT, through a written agreement between the Business Unit and OUHSC IT, called a Customer Services Agreement.

Payment Card Data (PCI): Data that includes primary account number (PAN), full magnetic stripe data, CAV2/CVC2/CVV2/CID Codes, PIN/PIN Block.

Personally Identifiable Information (PII): Personally Identifiable Information (PII) is defined as an individual's 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

***Moderate Risk Information Systems*:** OUHSC has defined the following Information System types as moderate risk IS to the University.

- Web servers
- Database servers
- E-mail servers
- FTP servers
- Cloud service providers
- Excel files containing confidential data
- Access databases containing confidential data

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

5. Enforcement

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

6. Scope

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

7. Regulatory References

- FISMA Configuration Management Control Family
- HIPAA 45 CFR 164.308(a)(7)(ii)(E)
- 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

8. Policy Maintenance

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

9. Revision, Approval and Review

9.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	11/14/2005	OUHSC IT	Baseline Version
2.0	12/12/2014	OUHSC IT	Added new policy statements to reflect process requirements. Added clarification to the scope statement. Added classification table.
2.1	10/05/2015	OUHSC IT	Revised Purpose statement added "and data within their Business Unit" to the first sentence of the policy statement.
3.0	11/14/2016	OUHSC IT	Applied new policy template. Updated enforcement statement.
3.1	12/13/2016	OUHSC ISRB	See SharePoint for changes made on 12/13/16
3.2	04/04/2017	OUHSC IT	Added Category D – Workstation Applications Added identifiable research data to Category A. Updated regulatory references to include HIPAA and FISMA controls. Added S2 zone placements per category.
3.3	11/15/2017	OUHSC IT	Revised Animal Research Data examples to specify IACUC Protocol and Veterinary Records as Category B data.

9.2 Approval History

Version	Date	Approved By
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
3.2	09/12/2017	Information Security Review Board

3.2	11/6/2017	OUHSC Provost
3.3	12/12/2017	Information Security Review Board

9.3 Review History

Date	Reviewed By
10/05/2015	OUHSC IT
01/15/2015	ISRB
06/08/2016	OUHSC IT
11/14/2016	Legal Counsel
09/12/2017	OUHSC ISRB
11/6/2017	Provost