University of Oklahoma

Information Classification Standard

Standard ID:	001
Version:	2.0
Policy Owner:	Chief Information Officer
Policy Approver:	President, University of Oklahoma

PURPOSE

The Office of Information Technology Business Unit is responsible for developing and managing the University's strategy to prioritize Information Systems based on their classification, criticality, and business value.

This Standard reflects the University's commitment to identifying and implementing security controls that mitigate risks to Information and Information Technology (IT), to reasonable and acceptable levels. This Standard establishes the University's framework for classifying University Information. Classification of University Information will aid in identifying baseline security controls for the protection of the Information. The examples below are not exhaustive; users should contact the IT Governance, Risk and Compliance for assistance with classifying their Information, at grc@ou.edu.

SCOPE

This Standard applies to all Information generated by or for, owned by or for which the University is responsible, in support of the University's missions. University Information is information generated by or for, owned by, or otherwise in the possession of the University of Oklahoma that is related to the University's missions of higher education, research, and service. University Information may exist in any format (i.e. electronic, paper). Data Owners must classify information in accordance with the OU IT Information Classification standard statements.

STANDARD STATEMENTS

BASELINE CATEGORY

The University of Oklahoma has defined Category E – University Administrative and Financial Information as the default classification for all University Information, until otherwise classified as part of the System Security Assessment process.

INFORMATION TECHNOLOGY ADMINISTRATOR RESPONSIBILITIES

Information Technology Administrators must:

(i) Inventory all University Information Technology, and maintain an inventory list selected by the Business Unit, with the classification as described below.

CATEGORY A: HEALTHCARE DATA

Category A data includes data that is legally regulated by the Health Insurance Portability and Accountability Act of 1996, Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, and Children's Online Privacy Protection Act (COPPA). Category A data is also subject to State of Oklahoma Policy, Standards, Procedures, and Guidelines (PSPG).

DATA DESCRIPTION	EXAMPLES
Protected Health Information (PHI)	• Medical records • Health Insurance Plan information • Healthcare service payments
Human Participant Research Information	• ePHI identifiers, see University of Oklahoma HIPAA Policy, *De-Identification/Re-Identification of PHI.* • Treatment records
OU Health	• Medical records
Donor Information	• Medical information
Student Information	• Medical records

CATEGORY B: PAYMENT CARD DATA

Category B data includes data that is governed by Payment Card Industry (PCI) Data Security Standards to protect the confidentiality, integrity, and availability of the payment card data. Category B data is also subject to State of Oklahoma Policy, Standards, Procedures, and Guidelines (PSPG).

DATA DESCRIPTION	EXAMPLES
Payment Card Information	• Cardholder name • Credit/debit card account number • Credit/debit card expiration date • Credit/debit card verification number • Credit/debit card security code

CATEGORY C: STUDENT DATA

Category C data includes records that contain information directly related to a student, that are maintained by the University, and are governed by the Family Educational Rights and Privacy Act (FERPA), Higher Education Act of 1965, Gramm-Leach-Bliley (GLBA) Act, and Children's Online Privacy Protection Act (COPPA). Category C data is also subject to State of Oklahoma Policy, Standards, Procedures, and Guidelines (PSPG).

DATA DESCRIPTION	EXAMPLES
Student Data	• FERPA student records (including Student ID) • Access device numbers (card number, building access code, etc.) used to protect student records information • Class lists or enrollment information • Transcripts and/or student grade reports • Student assessments • Student graded and ungraded assignments • Student tests • Notes on student performance

	• Disciplinary action • Athletics or department recruiting information • Race/ethnicity information, including tribal affiliation • Date of birth • Gender/sex • Participation in campus activities and sports • Weight and height (athletics) • Dates of attendance • Status • Last name and first name or initial, with any one of the following: o Social Security Number o Driver's license number o State ID card o Passport number
Student Financial Information **(*requires additional data governance)**	• Financial Aid information • Financial information of students or parents • GLBA Loan or scholarship information • Payment history • Student tuition bills
Academic/Research Information	• Library transactions (e.g., circulation, acquisitions) • Library paid subscription electronic resources • Course evaluations
Donor Information	• Student donor information

CATEGORY D1: CONFIDENTIAL RESEARCH DATA

Category D1 research data includes data which the University is obligated to protect in accordance with the Department of Defense Cybersecurity Maturity Model Certification and National Institute of Standards and Technology (NIST) Special Publication 800-171. Category D1 data is also subject to State of Oklahoma Policy, Standards, Procedures, and Guidelines (PSPG).

DATA DESCRIPTION	EXAMPLES
Contracts and contract data referencing the labels	• Export Controlled Research or Information (ITAR) • Controlled Unclassified Information (CUI) • National Institutes of Health (NIH) • IACUC Protocol(s) • Animal Specimen Veterinary Records • For Official Use Only (FOUO) • Sensitive But Unclassified (SBU) • Limited Official Use (LOU) • Sensitive Unclassified Information (SUI) • Law Enforcement Sensitive • DEA Sensitive • Official Use Only (OUO) • Department Of Defense (DoD) Technical Information • Distribution Statements on Technical Documents • Sensitive Security Information • Protected Critical Infrastructure Information

	• Unclassified Controlled Nuclear Information • DFARS 252.204-7012

CATEGORY D2: RESEARCH DATA

Category D2 data includes research data generally planned for release or publish to the public, or data not under contractual or regulated obligations for data protection. Category D2 data is governed by the State of Oklahoma Policy, Standards, Procedures, and Guidelines (PSPG).

DATA DESCRIPTION	EXAMPLES
Business Data	• List of publications (published research) • Unpublished research or research detail/results that are not confidential data • Private funding information • De-identified research data
University Property	• Intellectual Property Disclosures • Unpublished know-how and/or data • Existing University Intellectual Property

CATEGORY E: UNIVERSITY ADMINISTRATIVE AND FINANCIAL DATA

Category E data includes confidential University information requiring security and privacy protection, subject to State of Oklahoma Policy, Standards, Procedures, and Guidelines (PSPG), Privacy Act of 1974, E-Government Act of 2002, and the Fair and Accurate Credit Transaction Act of 2003.

DATA DESCRIPTION	EXAMPLES
Business/Financial Data	• Financial transactions that do not include confidential data • Information covered by non-disclosure agreements • Contracts that do not contain PII • Credit reports • Records on spending, borrowing, net worth
University Property	• Proprietary intellectual property created by employees in connection with their work (patents, trademarks, copyrights, etc.) • Commercial license type agreements • Partner Agreements (NDA, Confidentiality, MTA, DUA, IPA, IIA, etc.)
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.) • Telephone/fax numbers, e-mail & employment information • Family information (spouse(s), partner, guardian, children, grandchildren, etc.)
Authentication Verifiers	• Passwords • Cryptographic private keys
Security/Safety Data	• Emergency operations procedures and planning documents • Facilities blueprints and utility documents • Power plant • OUPD data

	• Disaster Recovery and Business Continuity plans
Personal/Employee Data	• OU Employee ID Numbers • Income information and Payroll information • Personnel records, performance reviews, benefit information • Race/ethnicity information, including tribal affiliation • Gender/sex • Date and place of birth or age • Worker's compensation or disability claims • Last name and first name or initial, with any one of the following: o Social Security Number o Driver's license number o State ID card o Passport number o Federal Tax Information
Certain directory/contact information not designated by the individual 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
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, Standard and Procedures • Network diagrams • Technical blueprints • Security documentation and procedures • Licensed software/software license keys

CATEGORY F: PUBLIC DATA

Category F data includes data that the University is under obligation to make available to the public, and data for which there is no expectation of privacy or confidentiality. Category F data is also subject to State of Oklahoma Policy, Standards, Procedures, and Guidelines (PSPG).

DATA DESCRIPTION	EXAMPLES
Business Data	• Press Releases • Course information • Campus maps • Job postings • Official institutional reports, such as those required by law or accreditation

University Property	• Patent published applications • Issued Patent • Patent prosecution history

SUPPORTING POLICY AND STANDARDS

- Information Protection Policy
- Cybersecurity Policy
- Confidential Research and Publications Policy
- HIPAA Privacy/ Security Policies, https://apps.ouhsc.edu/hipaa/secured/default.asp
- IT Security policies, https://www.ou.edu/ouit/cybersecurity/policies/all-users

REFERENCES

- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Payment Card Industry (PCI) Data Security Standards
- National Institute of Standards and Technology Special Publication 800-171, Controlled Unclassified Information
- Gramm-Leach-Bliley Act (GLBA)
- Family Education Rights and Protection Act (FERPA)
- Higher Education Act of 1965
- Children's Online Privacy Protection Act of 1998 (COPPA)

ENFORCEMENT AND COMPLIANCE

Failure to comply with this standard or other applicable laws, policies, and regulations may result in the limitation, suspension, or revocation of user privileges and may further subject the user to disciplinary action including, but not limited to, those outlined in the Student Code, Staff Handbook, Faculty Handbook, and applicable laws. This policy is enforced by the OU Chief Information Officer. Internal Audit, or other departments charged with data security responsibilities, may periodically assess compliance with this policy and may report violations to the OU Board of Regents.

IT EXCEPTIONS

The CIO acknowledges that under rare circumstances certain cases will need to employ systems that are not compliant with this standard. Such instances must be documented using the IT Policy and Standards exception process by a Business or Process Owner owning the risk and approved in advance by an authorized IT Executive (an owner of the IT Policy that governs the policy/standard).

Table 1 Revision History

Revision Date	Version	Revised By	Changes Made
01/18/2019	1.0	OU IT Systems Security	Baseline Version
10/22/2019	1.0	OU IT GRC	Line 29, defined GRC abbreviation. Line 46 Business Impact, revised to reflect education services. Line 47 Business Impact, revised to reflect confidential research services. Line 49 Business Impact, revised to "operate services".
10/30/2019	1.0	OU IT GRC	Added to Page – Category C Examples: • Access device numbers (card number, building access code, etc.) used to protect student records information • Library paid subscription electronic resources Added to Page 4 – Category D1 Examples: • For Official Use Only (FOUO) • Controlled Unclassified Information (CUI) • Sensitive But Unclassified (SBU) • Limited Official Use (LOU) • Sensitive Unclassified Information (SUI) • Law Enforcement Sensitive • DEA Sensitive • Official Use Only (OUO) • Department Of Defense (DoD) Technical Information • Distribution Statements on Technical Documents • Sensitive Security Information • Protected Critical Infrastructure Information • Unclassified Controlled Nuclear Information • Export-Controlled Information • DFARS 252.204-7012 Added to Page 5 – Category D2 Examples: • De-identified research data
11/13/2019	1.0	OU IT GRC	Added "Treatment records" and "OU Clinical Enterprise" to the Category A examples. Added to Line 46, Control ID.AM-5-1: The University of Oklahoma has defined Category E – University Administrative and Financial Information as the default classification for all University Information. Information Protection requirements documented in the Category E – University Administrative and Financial Information Protection Standard must be applied at minimum for University Information Systems. Added "Student assessments", "Student assignments", and "Student tests" to the Category C examples.
12/06/2019	1.0	OU IT GRC	Added Supporting Policy and Standards Section
04/2021	2.0	OU IT GRC	Added GLBA to Category C Student Data with additional data governance requirements. Added Intellectual Property/University Property to Category D2, E and F. Clarified Student Graded and Ungraded Assignments.

Table 2 Approval History

Version	Approval Date	Approved by:
1.0	02/11/2020	Chief Information Officer

Table 3 Review History

Version	Review Date	Reviewed by:
1.0	10/22/2019	OU IT GRC for consolidation of comments.
1.0	10/01/2020	OU Data Governance Committee – Working Group (Susannah Livingood, Cliff Mack, Kevin Fitzgerald, Jennie Clary, April Dickson)
2.0	03/24/2021	Health Sciences Center IT Research Committee
2.0	04/27/2021	OU Data Governance Committee
2.0	04/28/2021	Office of Technology Development