Approved 8-24-2010

Rogers State University Ver. 1.0

Policy on IT System and Data Classification

POLICY STATEMENT

Data owners must identify all IT Systems and associated data, classify it according to the IT System and Data Classification Standards below and maintain an inventory of the IT Systems, data and the classification.

PURPOSE OF POLICY

This policy reflects the University's commitment to identify and implement security controls that mitigate risks to Information Technology Systems (ITS) to reasonable and acceptable levels. This policy establishes a framework for classifying institutional data based on its level of sensitivity, value and criticality to the University. Classification of data will aid in determining baseline security controls for the protection of data. The examples below are not exhaustive; users should contact the appropriate office (Legal Counsel, Admissions and Records, Financial Services, *etc.*) for additional information.

SCOPE

ENTITIES/INDIVIDUALS AFFECTED BY THIS POLICY

Any person or entity within or affiliated with Rogers State University that manages an IT System that processes, stores, transmits, and/or collects University data is responsible for complying with this policy.

RESOURCES AFFECTED BY THIS POLICY

This policy applies to all information, data, or systems owned by, or in custody of Rogers State University.

POLICY

ITS Owners must:

1. Identify all ITS and associated data
2. Classify all ITS and data according to the IT System and Data Classification Standards below

ITS Administrator is responsible for maintaining an inventory of all the ITS and the associated classification according to the ITS Owner.

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

To ensure the safety, reliability, and operations of University systems and to protect against the loss of University data, any ITS Owner using, storing, accessing, or in any way maintaining Category A: Regulated Data or Category B: Sensitive/Restrictive Data must coordinate with the Academic Computing Service (ACS) and implement any such policies or controls as directed. After consultation with ACS, if it is determined such implementation of policies or controls is infeasible, impractical, or unnecessary, the ITS Owner and IS shall develop policy and control exceptions detailing risk-mitigation efforts.

Category A: Regulated Data	
Description	• Data and ITS that is legally regulated to protect the confidentiality, integrity, and availability of the data, such as: HIPAA, PHI, PCI, PII, EAR, ITAR • Data or ITS that would provide access to confidential information • Data that has regulation that determines the requirements and penalties associated with release
Confidentiality	**Scope of access:** Intended access by as few users as possible and based on minimum necessary or least privilege. **Disclosure requirements:** May not be disclosed outside those allowed by role or responsibility to know.
Business Impact	Seriously impairs the functioning of the University or results in material financial, legal or reputational loss.

Examples *** exceptions apply**	**ITS or documentation of ITS with access to regulated 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 • Federal Tax Information • Financial account (checking, savings, brokerage, CD, etc.), credit card, or debit card numbers **Protected Health Information (PHI)** • Medical records • Payment information • Health Insurance Plan information **Business/Financial Data** • Credit card numbers with/without expiration dates
	Export Controlled materials

Category B – Sensitive/Restricted Data	
Description	Data or ITS should be classified as Sensitive/Restricted when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its affiliates. By default, all data or ITS that are not explicitly classified as Regulated or Public data should be treated as Sensitive/Restricted Data. Data that the ITS Owner and/or University executive leadership have determined not to publish or make public Data protected by contractual obligations
Confidentiality	**Scope of access:** Intended for access only by those with a need to know. **Disclosure requirements:** Requires documented permission of ITS Owner to disclose.
Business Impact	Significantly impairs the functioning of the University or results in significant financial, legal or reputational loss.

Examples *** exceptions apply**	**ITS 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 **Authentication Verifiers** • Passwords • Cryptographic private keys **Security/Safety Data** • Emergency operations procedures and planning documents • Facilities blueprints and utility documents • Power plant • RSUPD data • Disaster Recovery and Business Continuity plans **Personal/Employee Data** • RSU 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** • 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 **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 information (spouse(s), partner, guardian, children, grandchildren, etc.) • Medical information

	Management Data • Detailed annual budget information • Conflict of Interest Disclosures • University's investment information **ITS Asset Information** • Server Event Logs

	• Non-published Information Technology policy and procedures • Network diagrams • Technical blueprints • Security documentation and procedures

Category C – Public Data	
Description	• Data should be classified as public data when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates. • 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. • While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.
Confidentiality	**Scope of access:** Intended for public access. **Disclosure requirements:** May be freely disclosed without permission.
Business Impact	Negligible or limited operational, financial, legal or reputational loss.

Examples *** exceptions apply**	**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 activities and sports • Weight and height (athletics) • Dates of attendance • Status **Business Data** • Press Releases • Course information • Campus maps • Job postings • List of publications (published research)

REGULATORY REFERENCE

The following regulations were used to develop this policy.

- 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 ("GLBA")
- 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
- DFARS: Defense Federal Acquisition Regulation Supplement

Approval

Revisions and Approvals

Revisions

Revision Date	Version	Revised By	Changes made
8/20/2020	1.0	Brian Reeves	Creation

Approvals

Approval Date	Version	Approved By	Title

Review History

Version	Review Date	Reviewed By	Title

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.

Information Technology System (ITS): 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 ITS can reside on premise or off-premise.

ITS Sponsor (Executive Sponsor): an individual responsible for providing the necessary funding and support for the ITS Owner and Administrator to perform their roles and responsibilities. The ITS Sponsor provides executive oversight of data and/or ITS and assumes responsibility for policy compliance for the ITS under his or her control. The ITS Sponsor reviews high level risk items of the ITS and makes risk treatment decisions for the Business Unit.
ITS Owner (Business Owner): the individual responsible for classifying the data, establishing rules for disclosing and authorizing access to ITS data, conducting access control reviews, coordinating with campus IT to conduct risk assessments and serving as the escalation contact for the ITS Administrator.

ITS Owner Representative: An individual designated by the ITS Owner to act on his or her behalf.

ITS 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). The ITS Administrator is responsible for maintaining an inventory of all ITS and the association classification according to the ITS Owner. The ITS administrator role may be performed through an agreement between the business unit and Campus IT.

HIPAA: Health Insurance Portability and Accountability Act. A 1996 Federal law that restricts access to individuals' private medical information.

PHI: Protected Health Information. Individually Identifiable Health Information that is transmitted by, or maintained in, electronic media or any other form or medium

ITAR: International Traffic in Arms Regulations. The U.S. Department of State through the Directorate of Defense Trade Controls (DDTC) administers the International Traffic in Arms Regulations (22 CFR §§120-130), or "ITAR," which regulate items and information inherently military in design, purpose, or use. Referred to as "defense articles," such items are found on the U.S. Munitions List (USML), including technical data recorded or stored in any physical form, models, mockups, or other items that reveal technical data directly relating to items designated in the USML.

EAR: Export Administration Regulations. The U.S. Department of Commerce administers the Export Administration Regulations (15 CFR §§730-774), or "EAR," which regulate the export of "dual-use" items. These items include goods and related technology, including technical data and technical assistance, which are designed for commercial purposes, but which could have military applications, such as computers, aircraft, and pathogens.

PCI: Payment Card Industry. Credit card companies (such as Visa, MasterCard, and American Express) formed PCI in response the outbreak of credit card security breaches. These breaches diminished customer trust, so the PCI Council implemented a standard (called the Data Security Standard, or DSS) to assure consumers that credit card usage is still reliable and secure.

FERPA: The Family Educational Rights and Privacy Act (FERPA) affords students certain rights with respect to their education records. Faculty and Staff members must protect students' educational records in accordance with FERPA policies including when writing letters of recommendation for students or releasing student records to third parties such as parents or employers.