



Data Classification Policy

Approved by:

A handwritten signature in black ink, appearing to be "L. H. ...".

Date Approved:

3 24-09

Rogers State University
Data Classification Policy

I. Purpose

The purpose of the Data Classification Policy is to establish appropriate security controls that will be applied to the handling of university data according to its category. This policy will enable University personnel to determine the various types of data for which they are responsible, thus ensuring that proper measures are taken to protect the data.

II. Scope

This policy applies to faculty, staff, students, contractors, consultants, official university affiliates, and others who use the University's computing resources. These resources include all phone, video, and data communications. This policy applies to all equipment that is owned by Rogers State University.

III. Policy

Data can be divided into three (3) categories, according to the associated degree of confidentiality, as follows:

Category I: Public

Category I data is not sensitive or confidential. This category includes data that is meant for the public, as well as information that is not intended for the public but is not detrimental if disclosed to the public. Examples of Category I data include but not limited to:

- Course Catalogs
- News Releases
- Campus Maps

Category II: Sensitive

Category II data is sensitive data that is not otherwise protected by state and federal law or other regulations but that the University has an obligation to protect. This data is shared only among small groups who need access for the purpose of conducting University business. Examples of Category II data include but are not limited to:

- Data collected and utilized through research that is not Category III data
- Financial information that is not Category III data
- Confidential e-mails
- Phone directories
- E-mail addresses
- Birth Dates
- Bulk meta data

Category III: Protected

Category III data is the most sensitive data. This includes data that is protected by state and federal law. Rogers State University is required to comply with HIPAA, FERPA, PCI, and the Gramm-Leach-Bliley Act. Examples of Category III data include but are not limited to:

- Social Security Numbers
- Financial information, which includes credit card numbers, bank accounts, financial aid information, and bursar bills
- Medical Information
- Confidentiality Agreements
- Contracts
- Data collected and utilized through research grants