FERRIS STATE UNIVERSITY

BUSINESS POLICY

Data Classification Policy

Effective Date:	January 22, 2019
Policy Number:	2019: 06
Policy Owner:	Vice President, Administration and Finance
Supersedes:	2017:05

SCOPE

This policy applies to those who access, process, or store University data, including, but not limited to, all University employees, affiliates, student employees, students, vendors, emeriti, retirees, and contractors.

POLICY STATEMENT

Data Classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered, or destroyed without authorization. Data classification reflects the level of impact to the University if confidentiality, integrity or availability of the data are compromised. The classification of data also helps determine what security controls are appropriate. All University data are classified into one of three levels, or classifications as follows:

Confidential Data (Highest Sensitivity)

Data are classified as Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its affiliates. Confidential data are highly sensitive and may have personal privacy considerations, and are restricted by federal or state law. Examples of Confidential Data include student grades and financial aid data, social security and credit card numbers, and individuals' health information. The highest level of security controls is applied when technically feasible.

Restricted Data (Moderate Sensitivity)

Data are classified as Restricted when the unauthorized disclosure, alteration, or destruction of the data could result in a moderate level of risk to the University or its affiliates. Restricted Data are protected by University policy. By default, all University data that are not explicitly classified as Confidential or Public data should be treated as Restricted data. Examples of Restricted data include official University records such as financial reports, some human resources information, some research data, and budget information. Security controls will be in place to restrict access to the data.

Public Data (Lowest Sensitivity)

Data are 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. 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.

Public data are not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The impact of the institution should Public data not be available is typically low; inconvenient, but not debilitating. Examples of Public data include directory information, course information, and other information published on the Ferris.edu Internet website.

Note: The word "Public" used in data classification is defined differently than the word "public" used in State open records acts.

See Appendix A: *Examples of University Data Types Grouped by Classification* for more specific information.

Data Collections

Data Owners will assign a single classification to a collection of University information, in other words, a data collection, which is common in purpose or function. When classifying a data collection, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of a student's name, address and grades, the data collection must be classified as Confidential Data because one data element is considered Confidential.

Data Handling Requirements

For each classification, several data handling requirements are defined to appropriately safeguard the information. It is important to understand that overall sensitivity of University information encompasses not only its confidentiality but also the need for integrity and availability. Please refer to the *Data Handling Standards for All Users* document.

Violations/Sanctions

Suspected or known violations of this policy or applicable laws must be reported to Information Technology Services (TAC Service Desk), and if applicable, an employee's supervisor. Suspension of access to Ferris IT Resources may occur while a suspected violation is investigated. Any person found to have knowingly violated this policy will be subject to appropriate disciplinary action as defined by current University policy, student code of conduct, and/or collective bargaining agreements, or may have his or her access to Ferris IT Resources permanently removed. When appropriate, University authorities and/or law enforcement agencies may conduct an investigation into the incident.

DEFINITIONS

Data

Information collected, stored, transferred, or reported for any purpose, whether electronically or hard copy.

Data Owner

An individual with primary authority and accountability for specified information (e.g., a specific business function) or type of data. This individual has the ability to authorize or deny access to certain data. This individual is responsible for delegating responsibility to appropriate Data Users and ensuring the accuracy, integrity, and timeliness of the data.

Data User

An individual, with permission of the data owner, who may collect, store, transfer, or report data consistent with his or her function at the University.

University Information

Information collected, used, stored, reported, or presented in any format, on any medium, by any entity specified to be within the scope of this policy.

PROCEDURES

Access

Confidential and/or Restricted data must be controlled from creation to destruction. Access to Confidential and/or Restricted Data must be requested for an individual by their supervisor via the appropriate form(s), and then authorized by the Data Owner. Access to Confidential and/or Restricted data may be authorized to groups of persons by their job classification or responsibilities ("role-based" access), and may also be limited by one's department.

Please see the *Data Handling Standards for All Data Users* for other details related to working with University data.

RESPONSIBILITIES

The following list of responsibilities is not meant to be an exhaustive list. See the *Data Handling Standards for All Data Users* for more detailed information.

Data Users

- Protecting your account from any unauthorized access, including via mobile devices and web browsers. Do not share your ID or password with others.
- Protecting data you transmit or store by using a University approved method, particularly when it contains Confidential Data.
- Understanding what to do when you are made aware of a violation of this policy.

Department supervisors and managers, Data Owners

- Educating contractors, vendors, employees, including student employees, on how to comply with this policy.

Data Owner

- When a Privacy Officer has been assigned to a type or set of data (e.g. HIPAA, PCI DSS, FERPA, contracted data), the Data Owner is responsible for following the procedures determined by the assigned Privacy Officer.
- When a Privacy Officer has not been assigned, the Data Owner is responsible for setting the security classifications for University data, and developing procedures for creating, maintaining, and using University data, consistent with University policy and all applicable state and federal laws.

Data Security Administrator or Designee

- Specifies the information security controls for each level of data security classification. Assists Data Users in classifying their data that is not currently classified.

IT Staff

- Limiting their access to systems to: maintaining the system, supporting business users, investigating security or abuse incidents, and investigating violations of this or other University policies.
- Following all regulatory laws and requirements, and University account and systems management policies and procedures, and be aware of all related policies and procedures in effect in the departments they are working in.

CONTACTS

For questions about this policy, contact the Technology Assistance Center (TAC).
(231) 591-4822, or toll-free at (877) 779-4822.

APPENDIX A

Examples of University Data Types by Classification

RELATED INFORMATION/FORMS/INSTRUCTIONS

Links to Related Laws and Regulations

Family Educational Rights and Privacy Act (FERPA)
http://www.ed.gov/policy/gen/guid/fpco/ferap/index/html
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
http://www.hhs.gov/ocr/privacy/
Payment Card Industry (PCI)
https://www.pcisecuritystandards.org/pci_security/

Ferris Policies and other documents

Data Handling Standard for All Data Users
https://ferris.edu/htmls/administration/buspolletter/information/Data-Handling-Standards.pdf
Information Security Guidelines
http://ferris.edu/htmls/administration/buspolletter/Bpl0907InfoSecurityGuidelines.pdf
FERPA Staff Reference Sheet
http://ferris.edu/htmls/staff/forms/datasecurity/FERPA-Staff-Reference-Sheet.pdf

FERRIS STATE UNIVERSITY

Appendix A: Examples of University Data Types by Classification

The examples listed below are a sampling of those in each classification. This document is not meant to be an all-inclusive list. Please see the *Data Classification Policy* for further information.

Confidential (Highest Sensitivity)

This is information that is protected under State and/or Federal law.

Employee Data

Personally-Identifiable Information (PII) in any format (electronic, paper, report, etc.). Last name, and first name or initial, with any one of the following:

- Social Security Number (SSN)
- Driver’s license
- Passport number
- Race, ethnicity, and/or nationality, gender
- Financial account number (checking, savings, brokerage, CD, credit and debit cards, etc.)
- Date of Birth
- Background check results
- Salary/payroll information (W-2, W-4, Bulldog Card info, union dues, etc.)
- Personnel records, performance reviews, benefit information

Payroll information (garnishments, child support, separation agreements, etc.)
OSHA reportable information
Worker’s compensation or disability claims
Ferris corporate card numbers
Passwords/PIN numbers

Student Data

Note: All information is confidential for a student with a Confidentiality Indicator in Banner

Family Educational Rights and Privacy Act (FERPA): Refer to *FERPA Staff Reference Sheet* for details.

- Academic status
- Date of birth (may be different for athletic eligibility use)
- Mass mailing of email address (The University will not use email addresses for third party commercial uses)
- Gender
- Race/Ethnicity
- Grades
- Grade Point Average (GPA)
- Nationality
- Student Identification/ID Card Photographs (exception made for University sports photos)
- Residency status

- Student’s class schedule
- Social Security Number (SSN)
- Test scores
- Universal Indicator Code (UIC)

Student background check information
Student misconduct files/Student Judicial Services files
Student and parent financial aid information
NCAA documentation
SEVIS/immigration information
Passwords/PIN numbers

Health Insurance Privacy and Accountability Act (HIPAA) Patient Information

- Name
- Geography (Zip Code, city)
- Dates (birth, admitted)
- Phone
- Fax
- Email information
- Social Security Number (SSN)
- Medical ID
- Health plan ID
- Account numbers
- Certificate numbers
- License plate/VIN
- Device IDs or serial numbers
- URLs
- IP address
- Biometrics
- Facial photographs
- Any other unique ID (diagnosis code, etc.)

Other Information

- Library transactions (e.g., circulation, etc.)
- Public Safety’s case information
- Vendor information with SSN or Confidential information
- Audit logs
- IT system event data
- Data incident/breach information
- IT infrastructure information (firewall/network)
- General Counsel’s case information
- IT system configuration information

All other credit card information (PCI data)

Restricted (Moderate Sensitivity)

This is information protected by University policies, procedures, or agreements.

Employee Data

- Employee Campus-Wide ID (101*xxxxx*)
- Directory/contact information designated by the owner as "Private"
- Programming code

Student Data

- Student Campus-Wide ID (101*xxxxx*)

Business/Financial/Management Data

- Financial transactions which do not include confidential data
- Contracts that do not contain PII
- University's credit report
- Records on spending, borrowing, net worth
- Budget account numbers
- Conflict of Interest disclosures
- University building blueprints

Academic/Research Information

- Unpublished research or research detail/results that are not confidential data
- Private funding information
- Aggregate human subject information
- Course evaluations

Donor Information

Last name and first name or initial (and/or name of organization, if applicable) with any of the following:

- Telephone/fax numbers, address, email, employment information
- Family information (e.g., spouses, partner, guardian, children, grandchildren, etc.)

Anonymous Donor Information (This information is released to authorized personnel only)

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)

Public (Lowest Sensitivity)

Directory information not previously listed

- Campus maps
- Job postings
- List of publications/published research
- Sports-related photography