FERRIS STATE UNIVERSITY

Data Handling Standards for All Data Users

Effective Date:	January 22, 2019
Document Number:	2019: 05
Document Owner:	Vice President, Administration and Finance
Supersedes:	October 17, 2016

SCOPE

These standards apply to anyone who accesses, processes, or stores University data, including, but not limited to, all University employees, affiliates, student employees, students, vendors, emeriti, retirees, and contractors.

The handling of information is viewing, using, updating, deleting or destroying data. These standards are in effect for handling data whether at rest, in use, or in transit. Data can be in paper or electronic form. The *Data Classification Policy* identifies types of data (Confidential, Restricted, or Public) and this document states how the data must be handled based on the classification.

STANDARDS STATEMENT

Introduction

These handling requirements apply to University data whether the data are at rest, in use, or in transit and represent the minimum requirements for handling of data in any format. Individual areas may establish more stringent data handling requirements.

Data are classified into three types: confidential (highest sensitivity), restricted (moderate sensitivity), or public (lowest sensitivity). Please view the *Data Classification Policy* for a list of additional details on predefined University data.

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 institutional data encompasses confidentiality, integrity, and availability of data.
The following table defines required safeguards for protecting data based on classification. In addition to the following data security standards, any data covered by federal laws, state laws, regulations, or contractual agreements must meet those security requirements. If you are working with non-Ferris data (for example, from another university or contracted vendor), you must follow their data handling policies and procedures. As part of proper data handling processes, please refer to your department's schedule developed in accordance with the *University Records Management Policy.*

All Data Users

Security Control Category	Data Classification		
	Public (lowest sensitivity)	**Restricted (moderate sensitivity)**	**Confidential (highest sensitivity)**
Copying/Printing - applies to both paper and electronic media	• No restrictions	• Data should only be printed when there is a legitimate need • Copies must be limited to individuals with a need to know • May be sent via University Mail • Do not leave unattended where others may see it • Unauthorized access to materials must be prevented by locking doors, cabinets, etc.	• Data should only be printed when there is a legitimate need • Copies must be limited to individuals authorized to access the data and have signed a Ferris Employee Confidentiality Agreement • Copies must be labeled "Confidential" • Must be sent via Confidential envelope • Do not leave unattended where others may see it • Unauthorized access to materials must be prevented by locking doors, cabinets, etc.
Physical Data Security - protection from physical circumstances and events that can cause data loss or damage	• Computer or device should be locked or logged out when unattended	• Computer or device screen must be locked, or user logged out, when unattended • Privacy screens for computer display where feasible • Unauthorized access to materials must be prevented by locking doors, cabinets, etc.	• Computer or device screen must be locked, or user logged out, when unattended • Privacy screens for computer displays if others might be able to see your screen • Unauthorized access to materials must be prevented by locking doors, cabinets, etc.

Security Control Category	Data Classification		
	Public (lowest sensitivity)	**Restricted (moderate sensitivity)**	**Confidential (highest sensitivity)**
Data Storage - protecting digital media used to retain data on network devices and systems (e. g., servers, laptops, desktops, tablets, removable media – thumb drives, external hard drives, etc.) - backup and security is only provided on IT managed or University approved storage identified within this standard	• IT managed or University approved data storage (e.g., H:, J: network drives, local device storage, and removable storage–including Office 365 cloud storage). Multi-Factor Authentication* is recommended but not required for this classification. • IT or designee performs risk assessment • Follow your department's University Records Management Policy/schedule	• IT managed or University approved data storage (e.g., H:, J: network drives, local device storage, and removable storage~~,~~ including Office 365 cloud storage. Multi-Factor Authentication* is required for data classified as Restricted if using Office 365 cloud storage. • Full Disk Encryption (FDE) and File and Folder Encryption (FFE) recommended, where technically feasible and is based on security risk assessment • IT or designee conducts risk assessment • Follow your department's University Records Management Policy/schedule	• IT managed or University approved data storage (e.g., H:, J: network drives, local device storage, and removable storage, including Office 365 cloud storage. Multi-Factor Authentication* is required for data classified as Confidential if using Office 365 cloud storage. • Full Disk Encryption (FDE) and File and Folder Encryption (FFE) required, where technically feasible and is based on security risk assessment • Encryption on backup media required • IT or designee conducts risk assessment • Follow your department's University Records Management Policy/schedule

- *Multifactor authentication (MFA) is a security system that requires more than one method of authentication to verify the user's identity for login. Multifactor authentication combines two or more independent credentials: what the user knows (password) and what the user has (security token). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access Ferris State University systems and data.

Security Control Category	Data Classification		
	Public (lowest sensitivity)	**Restricted (moderate sensitivity)**	**Confidential (highest sensitivity)**
Transmission - protecting the data when traversing network communication medium	• Use up-to-date encrypted protocols recommended (e.g. Hypertext Transfer Protocol-Secure (HTTPS), Secure File Transfer Protocol (SFTP), Secure Shell (SSH))	• Transmission of Restricted Data through any non-Ferris network (wired or wireless) is strongly discouraged. Where possible use the University's Virtual Private Network (VPN) is recommended • Use up-to-date encrypted protocols required (e.g. Hypertext Transfer Protocol-Secure (HTTPS), Secure File Transfer Protocol (SFTP), Secure Shell (SSH)) where technically feasible	• Transmit via encrypted email • Use of a digital signature in email is recommended • Use of the University's Virtual Private Network (VPN) required • Paper should be in a locked container • Use up-to-date encrypted protocols required (e.g. Hypertext Transfer Protocol-Secure (HTTPS), Secure File Transfer Protocol (SFTP), Secure Shell (SSH)) where technically feasible
Mobile Device Configuration - e.g., cell phones, tablets, and laptops	• Password or PIN protection is recommended • Locked and secured when unattended	• Must have a password or PIN, and locked when not in use • ITS managed full disk encryption (FDE) recommended where technically feasible and is based on security risk assessment • ITS managed Mobile Device Management (MDM) is recommended	• Must have a password or PIN, and locked when not in use • ITS managed full disk encryption (FDE) required where technically feasible and is based on security risk assessment • ITS managed Mobile Device Management (MDM) is recommended
Disposal - secure removal and destruction of data e.g., on hard drives, removable storage, CDs, DVDs, media cards, tapes, paper, etc.	• Recycling paper copies is recommended • Wipe/erase media recommended	• Shredding of paper copies is required • Wipe/erase media according to TAC Asset Lifecycle Management's procedures required	• Shredding of paper copies is required • Wipe/erase/destroy media according to TAC Asset Lifecycle Management's procedures required

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 University 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, Code of Student Community Standards, and/or collective bargaining agreements. Their access to University IT Resources may also be permanently removed. When appropriate, University authorities and/or law enforcement agencies may conduct an investigation into the incident. Legal action may be taken when federal or state laws or other regulations have been violated.

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. He or she 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, manipulated, stored, reported or presented in any format, on any medium, by any unit of the University.

RESPONSIBILITIES

The following list of responsibilities is not meant to be exhaustive. See the *Information Security Guidelines* 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.

Data Owners and Privacy Officers

- Educating data users on how to comply with this policy.
- When a Privacy Officer has been assigned for a type or set of data (e.g., HIPAA, PCI DSS, FERPA, contracted data), the Data Custodian is responsible for following the procedures determined by the assigned Privacy Officer.
- When a Privacy Officer has not been assigned, the Data Custodian 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.

IT Staff

- Limiting their access to data to: maintaining the system, investigating security or abuse incidents, and investigating violations of this or other University policies.
- Following all privacy and account management policies and procedures established by the University, and be aware of all related policies and procedures in effect in the departments they are working in.

University Data Security Administrator or Designate

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

PROCEDURES

Training

All users need to be trained to properly handle data. Users who have access to restricted and confidential data will receive online security training. As per government/Industry regulation and compliance requirements, employees handling confidential data will receive data handling and classification training. Training will be provided via New Employee Orientation, Cyber Security training sessions, and online security awareness sessions.

Auditing

Auditing includes the examination of the data and user management controls within an information technology infrastructure. Auditing of data classified as Public data is not needed. For Restricted Data, logins of success and failure attempts to systems are audited, and we will follow government and industry regulatory/compliance requirements. For Confidential Data, logins of success and failure attempts to systems, as well as access and changes to objects, will be audited. We will follow government and industry regulatory/compliance requirements related to Confidential Data.

CONTACTS

Contact the Information Technology Solution Center (ITSC) Service Desk for any questions at (231) 591-4822 or (877) 779-4822.

RELATED INFORMATION/FORMS/INSTRUCTIONS

Related Laws

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 Data Security Standards (PCI-DSS)
https://www.pcisecuritystandards.org/pci_security/

Ferris Policies and References

Data Classification Policy
https://ferris.edu/htmls/administration/buspolletter/information/data-classification-policy.pdf
Information Security Guidelines
http://ferris.edu/htmls/administration/buspolletter/Bpl0907InfoSecurityGuidelines.pdf
Student Affairs FERPA Sheet for Staff
http://www.ferris.edu/htmls/staff/forms/datasecurity/FERPA-Staff-Reference-Sheet.pdf
University Records Management Policy
http:/ferris.edu/htmls/administration/buspolletter/Bpl1006.pdf