FORT HAYS STATE UNIVERSITY
Forward thinking. World ready.

University Policies
www.fhsu.edu/policies/

POLICY TITLE: Data Classification Policy

POLICY PURPOSE: Data and information are important assets of the university and must be protected from loss of confidentiality, integrity, or availability in compliance with FHSU policies, Board of Regents policy, and state and federal laws and regulations.

BACKGROUND: A hierarchal Information Asset classification standard is required by KITEC Information Technology Policy 7230A and is also important to ensure compliance with the Family Educational Rights and Privacy Act of 1974 (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach-Bliley Act (GLBA), and other federal and state laws and regulations.

APPLIES TO: All university data.

DEFINITIONS: **University data:** Electronic information providing support to and meeting needs of the University community. Data includes, but is not limited to:

- Elements supporting financial management;
- Student records;
- Payroll;
- Personnel records;
- Capital equipment inventory; and,
- Any electronic information:
  - Used for planning, managing, reporting, or auditing a major administrative function;
  - Referenced or used by a Department(s) or College(s) to conduct University business;
  - Included in a University administrative report; or,
  - Used to derive a data element meeting any of the criteria above.

CONTENTS:

Contents

POLICY STATEMENT:

Roles and Responsibilities

Everyone with any level of access to University Data has responsibility for its security and is expected to observe requirements for privacy and confidentiality, comply with protection and control procedures, and accurately present the data in any type of reporting function. The following roles have specific responsibilities for protecting and managing University Data.

Chief Data Steward - Senior administrative officers of the university responsible for overseeing all information resources (e.g., the Provost and Vice Presidents).

Data Steward - Deans, associate vice presidents, and heads of academic, administrative, or affiliated units or their designees with responsibility for overseeing a collection (set) of University Data. They are in effect the owners of the data and therefore ultimately responsible for its proper handling and protection. Data Stewards are responsible for ensuring the proper classification of data and data collections under their control, granting data access permissions, making sure people in data-related roles are properly trained, and ensuring compliance with all relevant polices and security requirements for all data for which they have responsibility.

Data Manager - Individuals authorized by a Data Steward to provide operational management of a University Data collection. The Data Manager will maintain documentation pertaining to the data collection (including the list of those authorized to access the data and access audit trails where required), manage data access controls, and ensure security requirements are implemented and followed.

Data Processor - Individuals authorized by the Data Steward or designee and enabled by the Data Manager to enter, modify, or delete University Data. Data Processors are accountable for the completeness, accuracy, and timeliness of data assigned to them.

Data Viewer - Anyone in the university community with the capacity to access University Data but not to enter, modify, or delete it.

Information Security Officer - Provides advice and guidance on information and information technology security policies and standards.

Internal Audit Office - Performs audits for compliance with data classification and security policy and standards.

Data Classification Scheme

Data assets shall be classified in a manner consistent with its value and sensitivity to loss or disclosure.

Data will be protected according to the FHSU Data Security Standard.

Each data element and data view of University data will be assigned one of the following three classifications by the Data Stewards, in consultation with the Chief Data Steward to whom they report:

1. **Public** - Data explicitly or implicitly approved for distribution to the public without restriction. It can be freely distributed without potential harm to the University, affiliates, or individuals. Public data generally have a very low sensitivity since by definition there is no such thing as unauthorized disclosure, but it still warrants protection since the integrity of the data can be important. Examples include:
    1. FHSU's public web site.

2. Directory information for students, faculty, and staff except for those who have requested non-disclosure (e.g., per the Family Educational Rights and Privacy Act (FERPA) for students).
3. Course descriptions.
4. Semester course schedules.
5. Press releases.

2. **Internal** - Data intended for internal University business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. Internal data are generally not made available to parties outside the FHSU community. Unauthorized disclosure could adversely impact the University, affiliates, or individuals. Internal data generally have a low to moderate sensitivity. Examples include:
    1. Financial accounting data that does not contain confidential information.
    2. Information technology transaction logs.
    3. FHSU ID number.
    4. Student educational records.
    5. Directory information for students, faculty, and staff who have requested non-disclosure (e.g., per FERPA for students).
3. **Restricted-Use Information**- Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization by the Data Steward is required for access because of legal, contractual, privacy, or other constraints. Unauthorized disclosure could have a serious adverse impact on the business or research functions of the University or affiliates, the personal privacy of individuals, or on compliance with federal or state laws and regulations or University contracts. Restricted-Use Information has a very high level of sensitivity. Examples include:
    1. Social Security Number.
    2. FERPA protected student data.
    3. Credit card number.
    4. Passport number.
    5. Personnel records.
    6. Medical records.
    7. Authentication tokens (e.g., passwords, biometric data).
    8. Personal identity information (PII) as defined by K.S.A. § 21-6107: Crimes involving violations of personal rights. This includes, but not limited to: date of birth; driver's license number or card or nondriver's identification number or card; place of employment; employee identification numbers or other personal identification numbers or cards; mother's maiden name; birth, death or marriage certificates; electronic signatures; and any financial number, or password that can be used to access a person's financial resources
4. **Proprietary Data** - Classification of data provided to or created and maintained by FHSU on behalf of a third party, such as a corporation or government agency, will vary depending on contractual agreements and/or relevant laws or regulations. The classification and security standards for proprietary data owned by the third party will be defined by the third party. Proprietary data owned by FHSU must be classified and protected according to FHSU's data classification policy and

security standards. Individuals managing or accessing proprietary data are responsible for complying with any additional requirements and security policies and procedures specified by the third party owner. Proprietary data include data classified by the federal government as Classified National Security Information (confidential, secret, top secret).

Unclassified Data

Unclassified data shall be treated as Restricted-Use Information.

Publically Accessible Data

Except as required by law or as designated by executive staff, data shall not be open to the general public.

Storing and Sharing Internal or Restricted-Use Information

Internal and Restricted-Use Information shall only be stored on FHSU file servers or within FHSU-provided applications or systems configured to securely store Internal or Restricted-Use Information.

Internal or Restricted-Use Information shall not be stored on a desktop or laptop hard drive, portable drive (flash drive, jump drive, CD, DVD, external drive, etc.), any non-approved cloud storage provider, or any personal equipment (including cell phones, laptops, and tablets).

Internal or Restricted-Use Information that needs to be transmitted outside of the FHSU network must be encrypted in transit and at rest. Regular email messages are not secure and must not be used to transmit anything other than public information.

Authentication is required to view, create, or edit Internal or Restricted-Use Information. System Users with access to Internal or Restricted-Use Information must be identified by a unique system identifier (username).

EXCLUSIONS OR SPECIAL CIRCUMSTANCES:

Amnesty Period for Departments and Individuals

Departments and individuals who are not following provisions of this policy, are expected to bring their practices into compliance with this policy within six months of its adoption by the President's Cabinet.

RELATED DOCUMENTS:

Policies:

Acceptable Use Policy

Email Policy

Endpoint Protection and Configuration Policy

Information Security Policy

Media Sanitization and Disposal Policy

Physical Security of Data Center and University Data Policy

Security Awareness Training Policy

Forms:

Other:

FHSU Data Security Standard

K.S.A. § 21-6107: Crimes involving violations of personal rights

Payment Card Industry Data Security Standard (PCI DSS)

Family Educational Rights and Privacy Act of 1974 (FERPA)

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Gramm-Leach-Bliley Act (GLBA)

Electronic Communications Privacy Act of 1986 (ECPA)

NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization

NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations

NIST Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories

Executive Order 12958: Classified National Security Information, As Amended, March 2003

KEYWORDS:	Data classification, public information, internal information, restricted-use information
RESPONSIBLE OFFICE:	Division of Technology Services
RESPONSIBLE UNIVERSITY OFFICIAL:	Director of Technology Services
ORIGINATION DATE:	3/2017
REVIEW CYCLE:	Every 3 years

POLICY ADDRESS:	
LAST APPROVED ON:	Adopted by ELT on 6/19/2017
REVIEW/CHANGE HISTORY:	Adopted by ELT on 3/31/2017
NEXT REVIEW DATE:	6/2020