SOUTHEAST MISSOURI STATE UNIVERSITY · 1873	BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 9/17	Revision Date: 12/23	Page: 1 of 5 Classification Code: 10-03
		Section: INFORMATION TECHNOLOGY		
		Subject: INFORMATION SECURITY		

GENERAL STATEMENT OF POLICY

Electronic Data refers to any data stored, processed, or transmitted electronically, including but not limited to, personal, financial, and academic information. The University is committed to protecting the privacy and security of its Electronic Data by implementing appropriate safeguards and adhering to data stewardship principles.

This policy defines information classifications and assigns responsibility for ensuring information privacy and security at each level of access and control. Information classification, in the context of information security, is the classification of information based on its level of sensitivity and the impact to the University should that information be disclosed, altered or destroyed without authorization. The classification of information helps determine what baseline security controls are appropriate for safeguarding that information.

All University information is categorized into one of five classification levels. In cases where information may fall into more than one classification, the highest applicable classification will apply.

DEFINITIONS

1. **Campus Secured:** A category of University data that the University has classified as not for public consumption but unlikely to cause material harm to the University if lost, leaked, or destroyed**.**

2. **Card Verification Value (CVV):** A three or four digit code, depending on the credit card, is a number used to verify physical access to a credit or debit card.

3. **Data Custodian:** A data custodian is responsible for the proper storage, transport, aggregation, and business use of data.

4. **Data Owner:** A Data Owner is responsible for the classification, protection, use, and quality of specific campus data sets, as well as determining access permissions and ensuring compliance with relevant regulations, such as FERPA and PCI-DSS (see definitions below).

5. **Data Steward:** A Data Steward is responsible for ensuring the quality and accuracy of data, as well as compliance with data management policies for data stored by the University.

6. **Donor Records:** The name, address, phone number, email, or other information used to identify persons or organizations providing financial or other support to the university.

7. **FedRAMP:** The Federal Risk and Authorization and Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring.

8. **FERPA:** The Family Educational Rights and Privacy Act of 1974 (FERPA) is a US federal law that governs access to educational information and records.

9. **Financial Records:** Any information collected pertaining to expenditures, purchases, fees, salaries, or account balances including account numbers, routing numbers, and some credit card information such as the PAN or CVV.

Commented [SB1]: Explain these acronyms.

10. **Material Harm:** A category of University data that the University has classified as likely to cause harm to individuals or to the University if lost, leaked, or destroyed.

11. **PCI:** PCI or PCI-DSS is the security standard framework created by the Payment Card Industry (PCI). It is a framework mandated by the payment card industry and is administered by the Payment Card Industry Security Standards Council.

12. **PHI:** Protected Health Information (PHI) consists of a combination of health and personal information aggregated to identify a specific individual. This includes,but is not limited to, data such as medical record numbers, patient names, email addresses, and x-rays.

13. **PII:** Personally Identifiable Information (PII) is information that, used separately or aggregated with additional information, can identify a specific individual.

14. **Primary Account Number (PAN):** A number consisting of 14 to 19 digits on a credit card that acts as the unique identifier of the debit or credit card.

15. **Public Information:** The least sensitive category of University data that the University has classified as public information that is easily accessible to the general population or intended to be disseminated to the public and would not cause harm if lost, leaked, or destroyed.

16. **Serious Harm:** A category of University data that the University has classified as highly likely to cause serious harm to individuals or to the University if lost, leaked, or destroyed.

17. **Severe Harm:** The most sensitive category of University data that the University has classified as almost certain to cause severe, possibly irrevocable harm to the University if lost, leaked, or

destroyed.

18. **Sunshine Laws:** A series of laws and regulations which require public disclosure of government meetings and records to maintain transparency with the public.

POLICY SCOPE

1. **Category 1: Public Information**

   Public Information data consists of data easily accessible to the general population or intended to be disseminated to the public, including:

   - Information published on a non-secured website
   - The only data that can be posted on university social media sites (Facebook, Twitter, etc.)
   - Course catalogs
   - Staff and faculty directory information
   - Event dates or speakers

2. **Category 2: Campus Secured**

   Campus Secured data is classified by the University as not for public consumption but unlikely to cause material harm to the University, including:

   - Building plans or blueprints
   - Information regarding the University physical plant
   - Memos, letters or private campus, business-specific correspondence

3. **Category 3: Material Harm**

   Data in the Material Harm data category is classified by the University likely to cause harm to individuals or the to University if leaked, lost, or destroyed. Examples of this data include:

   - Information protected under Federal FERPA regulations
   - Campus financial records
   - Donor Information

4. **Category 4: Serious Harm**

   Data in the Serious Harm category is classified by the University as highly likely to create serious harm to individuals or to the University if leaked, lost, or destroyed. Examples of this data include:

   - Faculty, staff, or student financial information including personal credit card or bank account numbers
   - Social Security numbers
   - Credit card or bank account numbers
   - Passwords to financial or health websites or services

5. **Category 5: Severe Harm**

   Data in the Severe Harm category is classified by the University as almost certain to cause severe, possibly irrevocable harm to the University if leaked, lost, or destroyed. Examples of this data include:

   - Research conducted as part of a federal contract if protected under FedRAMP (such as data considered National Security information)

Information categorized at 3, 4, or 5:

- Should not be stored on or carried by mobile electronic devices or transmitted electronically unless the data is encrypted.
- Should not be transmitted to individuals external to the Southeast Missouri State University unless approved by the appropriate Data Steward.

The Information Security Officer (IS0) has authority to examine, or authorize examinations of, electronic mail messages, portable storage devices, files on desktops and laptops, web browser cache files, web browser bookmarks and other information stored on or passing through University computing resources when a data security incident is suspected.

University faculty, staff, and students are responsible for following governmental regulations and University guidelines for the retention and control of data to which they have access. Violations of this policy will be subject to disciplinary action up to and including termination of employment.

Data Stewards are those individuals responsible for University functions and who define and approve appropriate use and access of data within their areas of responsibility. Responsibilities include:

- Identification of valid data sources
- Rules, standards, and guidelines for the entry of new data, change of existing data, or deletion of data
- Rules, standards, and guidelines for controlled access to data
- Process for data integrity verification
- Acceptable methods for distributing, releasing, sharing, storing or transferring data
- Review and approval of access to restricted, confidential and internal data

Data Custodians are those individuals or departments providing operational support for an information system and having responsibility for implementing the data maintenance and control methods defined by the Data Steward. Responsibilities include:

- Acceptable methods for receiving data from identified sources
- Process for the verification of received data
- Providing for the security of restricted, confidential and internal data
- Assuring sound methods for handling, processing, security and disaster recovery of data