# 6.09 - INFORMATION CLASSIFICATION

**Effective:** August 15, 2024

**Purpose:** Emporia State University is committed to protecting the confidentiality, integrity, and availability of its information. This policy explains the requirements for classifying and protecting the University's data and information and defines responsibility for classification. This policy also establishes a framework for classifying University information as Confidential, Sensitive, and Public, so it can be protected and used appropriately. These classifications are based on both external requirements and University policies.

**Scope:** This policy applies to all members of the University Community. The policy applied to all information generated, accessed, modified, transmitted, stored, or otherwise used by the University Community.

University information exists on multiple forms of media (e.g., paper, hard drive, flash drive, cell phone, disk, DVD, or CD-ROM) and in many different formats (e.g., text, graphic, video, or voice; electronic or physical). All of these forms and formats of information require care and protection.

**Responsible Office**: Members of the Emporia State University community with specific responsibilities governed by this policy are listed below. For clarification on the terms used in this document, please refer to the policy on Security Policy Definitions. The Procedures for the Protection of University Information define the procedures required to fulfill these responsibilities.

Information Custodians are responsible for the classification of the University data under their stewardship.

Faculty are the personal custodians of their research and academic data and have the responsibility to classify the data under their stewardship.

Students are the personal custodians of their own data when such data is not owned by the University and is not part of their official academic record.

The University Information Security Officer assists the Information Custodian in classifying data, and ensures compliance with relevant laws, regulations, and policies, and establishes and implements procedures for the security of media and systems that store or transmit University data, based on the classification of that data. The Information Security Office (ISO) is responsible for monitoring and reporting compliance with this policy. The ISO is responsible for reviewing this policy annually. In all cases, information will be disclosed as required by controlling law.

**Policy Statement:** All University information shall be assigned to one of three classification levels:

- Confidential
- Sensitive
- Public

The default classification for all University Information, where an Information Custodian has assigned no other classification, is Sensitive. Information Custodians shall classify data under their stewardship, in consultation with the University Information Security team.

The term Information Custodian as used here does not imply ownership in any legal sense (i.e., holder of a copyright or patent). Information Custodians control and manage information on behalf of the University.

The Information Classification Standard provides a list of examples of data and their appropriate classification levels. This list is for illustrative purposes only, is not comprehensive, and is subject to change.

Any questions or concerns about the classification of University Information should be directed to the relevant Information Custodian or the University Information Security team.

<u>Confidential Information</u>

Information classified as Confidential has the potential to expose the University to significant risk. Therefore, it requires the most security methods of protection from unauthorized access, disclosure, or tampering. The Confidential classification applies:

- Because of legal or regulatory requirements, University policies or agreements to which the University is a party, or
- If unauthorized disclosure could result in significant risk to or adverse impact upon the University.

Due to the risks associated with the collection and storage or such information, Confidential information may only be collected when there is a specific business need for the information and no reasonable alternative exists.

Explicit authorization to download, transmit, or store Confidential information always requires approval by the University Information Security team. The University Information Security team must approve the storage of Personally Identifiable Information, especially Social Security Numbers, in any repository or system, prior to the creation of the system. Confidential information may only be disclosed to individuals on a need-to-know basis.

Confidential information must be stored on University managed resources, as it always requires significant protection from unauthorized access, tampering, or distribution. Physical media should be maintained in a locked cabinet within a locked office. Electronic data should be restricted by user login to “least privilege”, keeping access of information to

a need-to-know basis as required by an individual's job duties. The transmission of Confidential information requires it to be encrypted inside and outside of the University's trusted network, pursuant to the policy on Encryption. Destruction of information both physical and electronic should be performed in a manner consistent with the policy on Secure Disposal. Appropriate and required protections are established by the University Information Security team and defined in the Procedures for the Protection of University Information.

If information classified as Confidential is lost, disclosed to unauthorized parties, suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the University's information systems has taken place, or is suspected of taking place, members of the University Community are required to report the incident immediately, upon discovery of the known or suspected compromise, as described in the policy on Incident Response.

Sensitive Information

Information classified as Sensitive poses less risk than Confidential information, but is highly sensitive, and has the potential for significant negative impact to the University if disclosed and is restricted by policy or agreement to the members of the University Community.

Loss of Sensitive information could be harmful to the University's image, or reputation, or undermine the confidentiality of University business or processes. A loss of this type of information would not necessarily violate existing federal or local laws but would nonetheless pose substantial risk of disruption or negative impact.

Sensitive information must be stored only in authorized University systems, as it requires significant protection from unauthorized access or tampering. Physical media should be stored in a locked office. Electronic data should be restricted by user login to least privilege on a need- to-know basis as required by an individual's job duties. The transmission of Sensitive information requires it to be encrypted outside of the University's trusted network, pursuant to the policy on Encryption. Destruction of information both physical and electronic should be performed in a manner consistent with the policy on Secure Disposal. Appropriate and required protections are established by the University Information Security team and defined in the Procedures for the Protection of University Information.

If information classified as Sensitive is lost, disclosed to unauthorized parties, suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of the University's information systems has taken place, or is suspected of taking place, members of the University Community are required to report the incident within seventy-two (72) hours, upon discovery of the known or suspected compromise, as described in the policy on Incident Response.

Data Loss Prevention

Emporia State University utilizes Data Loss Prevention (DPL) technologies to assist in protecting Confidential and other regulated University information from unauthorized disclosures.

DLP is intended to complement, not replace, the responsibility of Information Custodians and University users. All members of the University community remain responsible for appropriately classifying, handling, and protecting University information in accordance with this policy.

The University's DLP solution may automatically identify and apply protective controls to electronic communications and files containing regulated information, including but not limited to:

- Family Educational Rights and Privacy Act (FERPA) protected information;
- Health Insurance Portability and Accountability Act (HIPAA) protected information;
- Payment Card Industry (PCI DSS) regulated information;
- Gramm-Leach-Bliley Act (GLBA) protected information; and
- Emporia State University and other institutional identifiers classified as Confidential.

When regulated information is detected in outbound communications, the University may automatically apply encryption or other security controls to reduce the risk of unauthorized disclosure.

Public Information

Public information can be freely disseminated to anyone and may be published on public web sites. While the requirements for protecting public data are less than that of Confidential and Sensitive information, sufficient controls must be maintained to protect against unauthorized modification of public information.

Appropriate and required protections for Public information are established by the University Information Security team and defined in the Procedures for the Protection of University Information.

ESU employees who knowingly violate the University's Information Classification Policy may be subject to disciplinary action, up to and including dismissal. Unauthorized access or disclosure of legally protected information may result in civil liability or criminal prosecution.

The President or designee must approve any exceptions to this policy.

**Definitions:** All words and phrases shall be interpreted utilizing their plain meanings unless otherwise defined in another University or Board of Regents policy or by statute or regulation.

**Procedures:** [Hyperlink to Information Technology procedures]

**Related Policy Information:** [Include here any supporting information for this policy]

**History**: Adopted: 10/20/2006 [FSB 06008 passed by Faculty Senate on 10/03/2006, approved by President, and included in UPM as Policy 3J.17]
Revised: 4/26/2019 [FSB 18015 passed by Faculty Senate on 04/16/2019 and approved by President]
Revised: 02/18/2020 [Removed from Faculty Senate]
Revised: 11/05/2020 [Updated and approved by ISAC]
Revised: 08/15/2024 [Policy format revised as part of UPM Revision]