# Data Classification Policy

*Information Technology*

## Purpose

The purpose of this policy is to establish a framework for classifying institutional data based on its level of sensitivity, value, regulatory requirements, and criticality to the University. Classification of data will aid in determining baseline security controls for the protection of data.

## Scope

This Policy applies to all employees, contractors, and third-party Agents of the University as well as any other University affiliate who is authorized to access Institutional Data.

## Definitions

- **Data Stewards:** University directors (typically at the level of Unit Director) who oversee data management functions related to the capture, maintenance, and dissemination of data for an operational area. They are responsible for decisions about the usage of University data under their purview.
- **Data Users:** Individuals and organizations that access institutional data and Information to perform their assigned duties or to fulfill their role in the University community.
- Institutional Data: All data owned or licensed by the University.

## 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. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All institutional data should be classified into one of three sensitivity levels, or classifications:

**A. Restricted Data**

- Data should be classified as Restricted when the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to the University or its affiliates. Examples of Restricted Data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted Data.

**B. Private Data**

- Data should be classified as Private when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to the University or its affiliates. By default, all Institutional Data that is not explicitly classified as Restricted or Public Data should be treated as Private Data. A reasonable level of security controls should be applied to Private Data.

**C. Public Data**

- Data should be classified as Public when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to the University and its affiliates. Examples of Public Data include press releases, course information, and research publications. 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.

An appropriate Data Steward should perform classification of data.

**Data Collections**

Data Stewards may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, 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 social security number, the data collection should be classified as Restricted even though the student's name and address may be considered Public Information.

**Reclassification**

On a periodic basis, it is important to reevaluate the classification of Institutional Data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the data or its value to the University. The appropriate Data Steward should conduct this evaluation. Conducting an evaluation on an annual basis is encouraged; however, the Data Steward should determine what frequency is most appropriate based on available resources. If a Data Steward determines that the classification of a certain data set has changed, an analysis of security controls should be performed to determine whether existing controls are consistent with the new classification. If gaps are found in existing security controls, they should be corrected in a timely manner, commensurate with the level of risk presented by the gaps.

**Calculating Classification**

The goal of information security, as stated in the University's Information Security Policy, is to protect the confidentiality, integrity, and availability of Institutional Data. Data classification reflects the level of impact to the University if confidentiality, integrity, or availability is compromised.

In some situations, the appropriate classification may be more obvious, such as when federal laws require the University to protect certain types of data (e.g., personally identifiable information). If the appropriate classification is not inherently obvious, consider each security objective using the following table as a guide. It is an excerpt from Federal Information Processing Standards ("FIPS") publication 199 published by the National Institute of Standards and Technology, which discusses the categorization of information and information systems.

| | POTENTIAL IMPACT | | |
|---|---|---|---|
| **Security Objective** | **LOW** | **MODERATE** | **HIGH** |
| **Confidentiality**<br>Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. | The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Integrity**<br>Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. | The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |
| **Availability**<br>Ensuring timely and reliable access to and use of information. | The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. | The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. |

As the total potential impact to the University increases from Low to High, the classification of data should become more restrictive moving from Public to Restricted. If an appropriate classification is still unclear after considering these points, contact the Information Security Office for assistance.

## Questions

If you have questions or concerns regarding this policy or other Information Technology Security Policies, please contact the Office of Information Technology via phone: 386-822-7045, or email: support@stetson.edu.

## **Appendix A:** Predefined Types of Restricted Information

The Information Security Office has defined several types of Restricted Data based on state and federal regulatory requirements. They are defined as follows:

| | |
|---|---|
| **1.** | **Authentication Verifier** |
| | An Authentication Verifier is a piece of information that is held in confidence by an individual and used to prove that the person is who they say they are. In some rare instances, an Authentication Verifier may be shared amongst a small group of individuals. An Authentication Verifier may also be used to prove the identity of a system or service. Examples include, but are not limited to:<br>Passwords<br>Shared secrets<br>Cryptographic private keys |
| **2.** | **Payment Card Information** |
| | Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:<br><br>Cardholder name<br>Service code<br>Expiration date<br>CVC2, CVV2 or CID value<br>PIN or PIN block<br>Contents of a credit card's magnetic stripe |
| **3.** | **Personally Identifiable Education Records** |
| | Personally Identifiable Education Records are defined as any Education Records that contain one or more of the following personal identifiers:<br><br>Name of the student<br>Name of the student's parent(s) or other family member(s)<br>Social security number<br>Student number<br>A list of personal characteristics that would make the student's identity easily traceable<br>Any other information or identifier that would make the student's identity easily traceable |
| **4.** | **Personally Identifiable Information** |
| | For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:<br><br>Social security number<br>State-issued driver's license number<br>State-issued identification card number<br>Financial account number in combination with a security code, access code or password that would permit access to the account<br>Medical and/or health insurance information |

| 5. | **Protected Health Information ("PHI")** |
|---|---|
| | PHI is defined as "individually identifiable health information" transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium. PHI is considered individually identifiable if it contains one or more of the following identifiers:<br><br>Name<br>Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)<br>All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89)<br>Telephone numbers<br>Fax numbers<br>Electronic mail addresses<br>Social security numbers<br>Medical record numbers<br>Health plan beneficiary numbers<br>Account numbers<br>Certificate/license numbers<br>Vehicle identifiers and serial numbers, including license plate number<br>Device identifiers and serial numbers<br>Universal Resource Locators (URLs)<br>Internet protocol (IP) addresses<br>Biometric identifiers, including finger and voice prints<br>Full face photographic images and any comparable images<br>Any other unique identifying number, characteristic or code that could identify an individual |