The University of Oregon Data Classification Policy

Summary

All University data must be classified into defined access levels. Data may not be accessed without proper authorization.

The purpose of this policy is to protect the information resources of the University from unauthorized access or damage. The requirement to safeguard information resources must be balanced with the need to support the pursuit of legitimate academic objectives. The value of data as an institutional resource increases through its widespread and appropriate use; its value diminishes through misuse, misinterpretation, or unnecessary restrictions to its access.

Classification of Data

All University data must be classified into levels of sensitivity to provide a basis for understanding and managing University data. Accurate classification provides the basis to apply an appropriate level of security to University data. These classifications of data take into account the legal protections (by statute, regulation, or by the data subject's choice), contractual agreements, ethical considerations, or strategic or proprietary worth. Data can also be classified as a result of the application of "prudent stewardship", where there is no reason to protect the data other than to reduce the possibility of harm or embarrassment to individuals or to the institution.

Classification Levels

The classification level assigned to data will guide data owners, data custodians, business and technical project teams, and any others who may obtain or store data, in the security protections and access authorization mechanisms appropriate for that data. Such categorization encourages the discussion and subsequent full understanding of the nature of the data being displayed or manipulated. Data is classified as one of the following:

- **Public (low level of sensitivity)**
  Access to "Public" institutional data may be granted to any requester. Public data is not considered confidential. Examples of Public data include published directory information and academic course descriptions. The integrity of Public data must be protected, and the appropriate owner must authorize replication of the data. Even when data is considered Public, it cannot be released (copied or replicated) without appropriate approvals.
- **Internal (moderate level of sensitivity)**
  Access to "Internal" data must be requested from, and authorized by, the Data Owner who is responsible for the data. Data may be accessed by persons as part of their job responsibilities. The integrity of this data is of primary importance, and the confidentiality of this data must be protected. Examples of Internal data include purchasing data, financial transactions (that do not include sensitive data), information covered by non-disclosure agreements, and Library transactions.

- **Sensitive (highest level of sensitivity)**
  Access to "Sensitive" data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the University who require such access in order to perform their job, or to those individuals permitted by law. The confidentiality of data is of primary importance, although the integrity of the data must also be ensured. Access to sensitive data must be requested from, and authorized by, the Data Owner who is responsible for the data. Sensitive data includes information protected by law or regulation.

  In addition to the Sensitive classification, there are two subsections of Sensitive data.

  - **Regulated sensitive data** includes data governed by regulation such as FERPA, HIPAA, PCI-DSS, and GLBA. It is also governed by Federal, State, and Local law as well as contractual obligations.
  - **Unregulated sensitive data** includes data that is not legally regulated, but still considered sensitive due to proprietary, ethical, or privacy considerations.

Data Associated with Selected Regulations

Health Insurance Portability and Accountability Act (HIPAA)	Health Data
Family Educational Rights and Privacy Act (FERPA)	Student Data
Payment Card Industry Data Security Standard (PCI DSS)	Credit Card Data
Gramm-Leach-Bliley Act (GLBA)	Financial Data, Social Security Numbers

Data Security Recommendations for the Classification Levels

The Chief Information Security Officer will create and maintain security procedures for the various types of data use by the University. These are the **Minimum Security Procedure for Devices with Sensitive Information** and **Minimum Security Procedure for Devices with Public or Internal Information**. In addition, a security guide is available for the handling of physical data. This is the **Minimum Security Procedure for Handling Physical University Data**.

Roles and Responsibilities

Chief Information Security Officer

The Chief Information Security Officer implements policies and procedures to comply with the various regulation and laws applicable to the University of Oregon.

Data Trustees

Data Trustees are senior University officials or their designees who have planning, policy-level and management responsibility for data within their functional areas. Data Trustees responsibilities include:

- Assigning and overseeing Data Owners
- Overseeing the establishment of data policies in their areas
- Determining legal and regulatory requirements for data in their areas
- Promoting appropriate use and data quality

Data Owners

Data Owners are University officials having direct operational-level responsibility for the management of one or more types of data. Data Owners are assigned by the Data Trustee and are generally associate deans, associate vice presidents, directors or managers. Data Owner responsibilities include:

- The application of this and related policies to the systems, data, and other information resources under their care or control
- Assigning data classification labels using the University's data classification methodology
- Identifying and implementing safeguards for Sensitive Data
- Communicating and providing education on the required minimum safeguards for protected data to authorized data users and data custodians

In cases where multiple data owners collect and maintain the same Sensitive data elements, the data owners must work together to implement a common set of safeguards.

Data Custodians

Data Custodians are Information & Technology or computer system administrators responsible for the operation and management of systems and servers which collect, manage, and provide access to University data. Data Custodians must be authorized by the appropriate Data Owner. Data Custodian responsibilities include:

- Maintaining physical and system security and safeguards appropriate to the classification level of the data in their custody
- Complying with applicable University computer security standards
- Managing Data Consumer access as authorized by appropriate Data Owners
- Following data handling and protection policies and procedures established by Data Owners and Information Security

Data Consumers

Data Consumers are the individual University community members who have been granted access to University data in order to perform assigned duties or in fulfillment of assigned roles or functions at the University. This access is granted solely for the conduct of University business. Data Consumer responsibilities include:

- Following the policies and procedures established by the appropriate Data Owner and Information Security
- Complying with federal and state laws, regulations, and policies associated with the University data used
- Implementing safeguards prescribed by appropriate Data Owners for Sensitive Data
- Reporting any unauthorized access or data misuse to Information Security or the appropriate Data Owner for remediation