

## POLICY CONCEPT FORM

<b>Name and UO Title/Affiliation:</b>	Leo Howell, Chief Information Security Officer
<b>Policy Title/# (if applicable):</b>	Data Classification / IV.06.02
<b>Submitted on Behalf Of:</b>	Jessie Minton, CIO
<b>Responsible Executive Officer:</b>	Provost

---

**SELECT ONE:**  **New Policy**       **Revision**       **Repeal**

*Click the box to select*

**HAS THE OFFICE OF GENERAL COUNSEL REVIEWED THIS CONCEPT:**     **Yes**       **No**

If yes, which attorney(s): Bryan Dearing

### GENERAL SUBJECT MATTER

*Include the policy name and number of any existing policies associated with this concept.*

Data Classification Policy / IV.06.02

---

### RELATED STATUTES, REGULATIONS, POLICIES, ETC.

*List known statutes, regulations, policies (including unit level policies), or similar related to or impacted by the concept. Include hyperlinks where possible, excerpts when practical (e.g. a short statute), or attachments if necessary. Examples: statute that negates the need for or requires updates to an existing policy; unit level policy(ies) proposed for University-wide enactment; or existing policies used in a new, merged and updated policy.*

Minimum Security Procedure for Devices with Public or Internal Information – defines how to protect devices with data classified as Public or Internal.

<https://it.uoregon.edu/system/files/Minimum%20Security%20Procedure%20for%20Devices%20with%20Public%20or%20Internal%20Information.pdf>

Minimum Security Procedure for Devices with Sensitive Information - defines how to protect devices with data classified as Sensitive.

<https://it.uoregon.edu/system/files/Minimum%20Security%20Procedure%20for%20Devices%20with%20Sensitive%20Information.pdf>

---

## STATEMENT OF NEED

*What does this concept accomplish and why is it necessary?*

The current Data Classification Policy is being expanded to become the Information Asset Classification and Management Policy (IACMP). The IACMP expands the classification criteria from focusing on data confidentiality (sensitivity) to also include data integrity and availability. This provides better alignment with university needs and industry best practices to protect data confidentiality, integrity and availability (CIA). The IACMP also includes classification of devices that process, store or transmit data. It simplifies the current classification policy by reducing the number of levels from 4 to 3 – “Public, Internal, Sensitive-Regulated, Sensitive-Unregulated” to “Low Risk (green), Moderate Risk (amber), and High Risk (red). Finally, the policy expands the responsibilities of data stewards accountable for ensuring security of university data and compliance with legal requirements.

The new policy will provide a better foundation for the development of an overall university Data Security Framework (DSF) – see DSF Overview Document attached. This framework will consist of this policy, as well as: 1) Data Security Classification Table – provides a listing of university data types and their classifications as well as responsible Data Trustees, Data Stewards and Data Custodians; 2) Minimum Security Controls for Protecting Data and Systems by Classification - standards for administrative and technical requirements to protect University Data.

---

## AFFECTED PARTIES

*Who is impacted by this change, and how?*

All University users

---

## CONSULTED STAKEHOLDERS

*Which offices/departments have reviewed your concept and are they confirmed as supportive? (Please do not provide a list of every individual consulted. Remain focused on stakeholders (e.g. ASUO, Office of the Provost, Registrar, Title IX Coordinator, etc.).)*

<b>Name</b>	<b>Office</b>	<b>Date</b>
Julia Pomerenk	University Registrar	3/4/2019
Elaine Seyman	Law School Registrar	3/20/2019
Kaia Rogers, Sonia Potter	Human Resource	3/20/2019
Trisha Burnett	Internal Audit	3/27/2019

Adriene Lim, Helen Chu	University Libraries	3/22/2019
Wendy Machalicek	Special Education and Clinical Sciences	3/22/2019
Mike Andreasen	University Advancement	4/2/2019
Lalla Pudewell	HEDCO Clinic	3/21/2019
Matthew Carmichael	UOPD	4/17/2019
Mike Harwood	Campus Planning & Facilities Management	4/9/2019
Kelly Wolf	Business Affairs Office	3/15/2019
Jessie Minton	Information Services	4/12/2019
Deb Beck, Alan Baker	University Health Center	4/17/2019
Sheryl Johnson	Research Compliance Services	4/8/2019
Chuck Williams, Orca Merwin	Innovation Partnership Services	4/8/2019
Elizabeth Denecke	Sponsored Projects Services	4/8/2019
Mary Kay Fullenkamp	Safety & Risk Services	4/1/2019
Debra McLaughlin	University Health Center	3/21/2019
Mahnaz Ghaznavi	Public Records Office	3/2019
Greg Shabram	PCS	4/19/2019
Information Security & Privacy Governance Committee (ISP GC)	University-wide	4/3/2019
IT Directors	University-wide	3/2019
<b>Other stakeholders scheduled for consultation before May 1 PAC meeting:</b>		
Paul Elstone, Lacie Larue, Maureen Procopio	University Advancement	
John Callahan, Jen Spry	UO Foundation	
Alisia Caban, Joseph DeWitz, Billy Ray	Counselling Center	

Andre Le Duc	Safety & Risk Services
Cassandra Moseley	Office of Research & Innovation
Jim Brooks	Scholarship and Financial Aid
Hilary Gerdes	Accessibility
Greg Skaggs, Jace Delaney	Athletics
Melanie Muenzer	Office of the Provost
Fred Sabb	Lewis Center for Neuroimaging
Eric Corwin	Physics

**POLICY**

*See attached*

Policy Staff Note: The **yellow highlights** indicate changes made post-PAC and **blue highlights** indicate changes made post-Senate (both meetings in May).

### **Reason for Policy**

This policy provides the University of Oregon’s approach for classifying data and information systems (“information assets”) according to their potential level of risk to the University. The policy and associated procedures also assign roles and responsibilities for protecting information assets and detail how such assets must be protected based on their classifications.

~~This policy will provide for a way for the UO Community to classify data according to its level of sensitivity. The associated procedures detail how classified data should be protected.~~

---

### **Entities Affected by this Policy**

All users of University of Oregon ~~data users~~information.

---

### **Web Site Address for this Policy**

(To be updated upon posting)

---

### **Responsible Office**

For questions about this policy, please contact the ~~Chief~~ Information Security Officer~~r~~ at 541-346-~~58379700~~ or ~~infosec@uoregon.edu wlaney@uoregon.edu.~~

---

### **Enactment & Revision History**

Enacted as a permanent policy by President Schill on April 25, 2016.  
Extended by President Michael Schill on December 15, 2015.  
Enacted as an emergency policy by Dr. Scott Coltrane, Interim President on June 25, 2015.  
This policy supersedes Fiscal Policy Manual 56.350.200-230 and UO Policy 10.00.01.

---

### **Policy**

#### **Summary**

The purpose of this policy is to outline the acceptable approach for classifying university information assets into risk levels to facilitate determination of access authorization and appropriate security control~~protect the information resources of the University from~~

~~unauthorized access or damage.~~ The requirement to safeguard information ~~resources/assets~~ must be balanced with the need to support the pursuit of ~~legitimate academic university~~ 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.

### **Definitions**

**Data Availability** refers to methods for ensuring that required data is always accessible when needed, in accordance with University retention policy.

**Data Confidentiality** refers to methods for ensuring that access to sensitive data is limited to authorized individuals.

**Data Integrity** refers to methods for ensuring that data is complete, accurate, consistent, and safeguarded from unauthorized modification.

**University Data** refers to data owned by or in the **legal** custody of the University, **regardless of source.** **Personally-owned data stored on University devices is not considered University Data.**

### **Classification of Data**

~~All University data is 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 or regulation), contractual agreements, ethical considerations, or strategic or proprietary worth. Data can also be classified as a result of the application of “prudent stewardship,” where the best reason to protect the data is to reduce the possibility of harm to individuals or to the institution.~~

=

### **Classification Levels**

~~The classification level assigned to data will guide Data Trustees, Data Stewards, 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)**

~~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 Data Trustee or Steward 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 Trustee or Steward 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), and information covered by non-disclosure agreements.~~

- ~~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 Trustee or Steward 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 state or federal law such as the

~~Family Educational Rights and Privacy Act, Health Insurance Portability and Accountability Act, Gramm Leach Bliley Act, and the Oregon Consumer Identity Theft Protection Act. It also may be governed by other federal, state, or local laws, or contractual obligations.~~

- ~~Unregulated sensitive data~~ includes data that is not regulated by statute, but still

~~considered sensitive due to proprietary, ethical, or privacy considerations. This generally includes all forms of research.~~

#### ~~Data Associated with Selected Regulations~~

~~Health Insurance Portability and Accountability Act (HIPAA): Personal Health Data~~

~~Family Educational Rights and Privacy Act (FERPA): Student Data (Education Records)~~

~~Payment Card Industry Data Security Standard (PCI DSS): Credit Card Data~~

~~Gramm Leach Bliley Act (GLBA): Financial Data, Social Security Numbers~~

~~Oregon Consumer Identity Theft Protection Act (CITPA): Social Security number, Driver license number, state identification number, Passport number/U.S. issued, identification number, Financial Data~~

#### ~~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~~

*Proposed redline – May 2019*

~~data. This is the Minimum Security Procedure for Handling Physical University Data. Finally, Information Services has developed an Employee Electronic Records Access Procedure.~~

## Roles and Responsibilities

### Chief Information Security Officer

The Chief Information Security Officer ~~implements~~ develops and implements policies and procedures to secure University information assets and comply with ~~the various~~ state, and federal, and international laws and regulations applicable to the University of Oregon.

### Data Trustee

The Data Trustee for all University ~~d~~Data is the Provost or their designees who have planning, policy-level, and management responsibility for data within their designated functional area(s). Data Trustees' responsibilities include:

- Assigning and overseeing Data Stewards.
- Overseeing the establishment of UO information asset data policies ~~in their areas~~.
- Determining statutory, and regulatory and other University requirements for UO information assets. ~~data in their areas~~
- Promoting data quality and integrity and appropriate use ~~and data quality~~.

### Data Stewards

Data Stewards are persons ~~University officials~~ members having direct operational-level responsibility for the management of one or more types of University data. Data Stewards must be authorized by the appropriate Data Trustee. Data stewards include, but is not limited to, and are generally associate deans, associate vice presidents or associate vice provosts, directors heads of departments, or above, or research principals, investigators or principal researchers for data they create or receive within the scope of work of their research project, instructors or students for data they create or receive within the scope of a work of their course of program or managers. Data Stewards' responsibilities include:

- Assigning and overseeing Data Custodians.
- ~~The application of this and related policies and procedures to the systems, data, and other information resources under their care or control.~~
- Assigning data classification levels in accordance with this policy and associated procedures ~~labels using the University's data classification methodology~~.
- Collaborating with the CISO in identifying and implementing appropriate administrative and technical safeguards outlined in the UO Minimum Information Security Controls Standard, for protecting information assets (see Related Resources, below). for Sensitive Data
- Collaborating with the CISO in communicating and providing education on the required minimum safeguards for protected data to authorized data-users and ~~d~~Data eCustodians.



***Proposed redline – May 2019***

- Authorizinge access, both logical and physical, only to authorized ~~personnel~~individuals who have a business need – as defined by law and university policies - to access specific data or other information assets.
- Authorizinge remote access to information assets to only ~~A~~authorized individuals ~~Personnel~~ who have a business need – as defined by law and university policies - to access ~~specific data~~ through a secured system approved by the Chief Information Security Officer ~~of the University~~.

In cases where multiple Data Stewards collect and maintain the same ~~sensitive~~ data elements, the Data Stewards must work together, in collaboration with the CISO, to apply the UO ~~Minium~~Minimum Information Security Controls, to implement a common set of safeguards.

**Data Custodians**

Data Custodians are ~~u~~University personnel or designated third-party agents ~~Information & Technology or computer system administrators~~ responsible for the operation and management of information systems ~~and servers~~ which collect, manage, process, or ~~and~~ provide access to University ~~d~~Data. Data Custodians must be authorized by the appropriate Data Stewards following procedures outline-d in the UO Minimum Information Security Controls Standard (see Related Resources, below). Data Custodians' responsibilities include:

- Applying the UO Minimum Information Security Controls ~~Maintaining physical and system security and safeguards~~ appropriate to the classification level of the data and other information assets in their custody.
- Complying with applicable University acceptable use and computer security policies, standards, and procedures.
- The application of this and related policies and procedures to the systems, data, and other information resources under their care or control.
- Managing Data Consumer access as authorized by appropriate Data Stewards.
- Following data handling and protection policies and procedures established by Data Stewards and the CISO ~~Information Security~~.

**Data Consumers**

Data Consumers are the individual University community members or third-party agents who have been granted access to University ~~d~~Data (wherever it is stored) in order to perform assigned duties or in fulfillment of assigned roles or functions for ~~at~~ the University. This access is granted solely for legitimate University purposes ~~the conduct of University business~~. Data Consumers' responsibilities include:

- Following the policies and procedures established by the appropriate Data Stewards, Data Custodians, and the CISO ~~Information Security~~;
- Complying with University policies and federal, international, and state laws and regulations, ~~and University policies~~ associated with the University ~~d~~Data and information system use ~~d~~;

***Proposed redline – May 2019***

- Implementing safeguards for protecting data as prescribed by appropriate Data Stewards and the CISO. ~~for Sensitive Data; and~~
- Reporting any unauthorized access or data misuse to ~~the~~ Information Security Office, as well as the appropriate Data Trustee, Steward, ~~and or~~ Custodian, for remediation.

A current list of UO Data Trustees, Data Stewards, and Data Custodians is available in the UO Data Security Classification Table (see ~~found below in~~ Related Resources, below).

### **Data Classification of Data**

Data Stewards must classify ~~A~~all University data – digital or printed - is classified into risk levels of sensitivity to provide ~~a~~the basis for understanding and managing University data. Accurate classification provides the basis to apply ~~applying an~~the appropriate level of security controls to University data. These classifications ~~levels consider the state and federal~~ of data take into account the legal protections (~~by statute or regulation~~), contractual agreements, ethical considerations, or strategic or proprietary worth. Data can also be classified as a result of the application of “prudent stewardship,” where the ~~best~~ reason to protect the data is to reduce the possibility of harm to individuals or to the institution.

### **Data Classification Levels**

The classification level assigned to data will guide Data Trustees, Data Stewards, Data Custodians, ~~business~~functional and technical project teams, and any others who may ~~create, obtain, process, transmit~~ 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 Stewards must classify University Data is classified as one of the following risk levels:~~

- **Public (low level of sensitivity) Low Risk (or Green)**

Data is classified as Low Risk if the loss of confidentiality, integrity, or availability of the data would have *minimal* strategic, compliance, operational, financial, or reputational risk to the University. ~~Public data is not considered confidential. Examples of Public data include published directory information and academic course descriptions. The integrity of Public~~Low Risk data is of primary importance and must be protected. ~~and the~~The appropriate Data Trustee or Steward must authorize ~~replication~~external release of the Low Risk data. Data already released in the public domain by University approved parties is considered “public data” and does not require further authorization for release. Refer to the UO Data Security Classification Table (see Related Resources, below) for examples of Low Risk data. ~~Even when data is considered Public, it cannot be released (copied or replicated) without appropriate approvals.~~

- **Moderate Risk (or Amber) Internal (moderate level of sensitivity)**

Data is classified as Moderate Risk if the loss of confidentiality, integrity, or availability

***Proposed redline – May 2019***

of the data would have *moderate* strategic, compliance, operational, financial, or reputational risk to the University. Integrity and availability of Moderate Risk data are of primary importance and must be protected; privacy and confidentiality should be protected as appropriate. Access to “Internal” Moderate Risk data must be requested from, and authorized by, the Data Trustee or Steward who is responsible for the data, as needed. Data access authorization may be provided to individuals may be accessed by persons as part of their job roles or 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), and information covered by non-disclosure agreements. Refer to the Data Security Classification Table (see Related Resources, below) for examples of Moderate Risk data.

- **High Risk (or Red) Sensitive (highest level of sensitivity)**

Data is classified as High Risk (the most sensitive/critical classification) if the loss of confidentiality, integrity, or availability of the data would have *high* strategic, compliance, operational, financial, or reputational risk to the University. Privacy, confidentiality, integrity, and availability are important and must be protected. Access to High Risk “Sensitive” data must be controlled from creation to destruction, and will shall 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 state or federal law. The confidentiality of data is of primary importance, although the integrity of the data must also be ensured. Access to sensitive High Risk data must be requested from, and authorized by, the Data Trustee or Steward who is responsible for the data.

High Risk Sensitive data includes information protected by law or regulation. Note: some data that is not regulated may be classified as High Risk by the Data Trustees or Stewards due to proprietary, ethical, or privacy considerations. Refer to the Data Security Classification Table (see Related Resources, below) for examples of High Risk data.

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

— Regulated sensitive data includes data governed by state or federal law such as the Family Educational Rights and Privacy Act, Health Insurance Portability and Accountability Act, Gramm–Leach–Bliley Act, and the Oregon Consumer Identity Theft Protection Act. It also may be governed by other federal, state, or local laws, or contractual obligations.

— Unregulated sensitive data includes data that is not regulated by statute, but still considered sensitive due to proprietary, ethical, or privacy considerations. This generally includes all forms of research.

### Data Associated with Selected Regulations

***Proposed redline – May 2019***

Health Insurance Portability and Accountability Act (HIPAA): Personal Health Data  
Family Educational Rights and Privacy Act (FERPA): Student Data (Education Records)  
Payment Card Industry Data Security Standard (PCI DSS): Credit Card Data  
Gramm Leach Bliley Act (GLBA): Financial Data, Social Security Numbers  
Oregon Consumer Identity Theft Protection Act (CITPA): Social Security number, Driver license number, state identification number, Passport number/U.S. issued, identification number, Financial Data

### **Classification of Information Systems and Technology Components**

Information systems and technology components, including computing and storage devices, mobile devices, network components, and applications, adopt the highest classification of the data that they process, store, or transmit. For example, a system that processes, stores, or transmits High Risk data is classified as a High Risk system; whereas a system that processes Moderate Risk data as the highest data classification level is classified as a Moderate Risk system.

In addition to data-specific risks, information systems components may also affect the safety of the UO community, through interference with operational technology (OT) such as building and industrial automated control systems and automation and supervisory control and data acquisition (SCADA) systems. An information system component is also classified as High, Moderate, or Low Risk if unauthorized access or modification or the loss of availability would have a high, moderate, or low safety risk respectively, to the UO community.

### **Data Security Recommendations Requirements for the Classification Levels**

The Chief Information Security Officer ~~will~~ shall create and maintain security procedures for the various types of data use by the University. These requirements are outlined in the UO [Minimum Information Security Controls standard \(see Related Resources, below\)](#). ~~Minimum Security Procedure for Devices with Sensitive Information and Minimum Security Procedure for Devices with Public or Internal Information.~~ Minimum Security Procedure for Devices with Sensitive Information and Minimum Security Procedure for Devices with Public or Internal Information. In addition, the CISO will create and maintain additional guidelines and procedures for appropriate handling of data including a security guide is available for the handling of physical data. This is the Minimum Security Procedure for Handling Physical University Data (see Related Resources, below). ~~Finally, Information Services has developed an Employee Electronic Records Access Procedure.~~

## **Related Resources**

**[UO Minimum Information Security Controls](#)**

**[UO Data Security Classification Table](#)**

**[Minimum Security Procedure for Devices with Sensitive Information](#)**

*Proposed redline – May 2019*

~~Minimum Security Procedure for Devices with Public or Internal Information~~

Minimum Security Procedure for Handling Physical University Data

~~Employee Electronic Records Access Procedure~~

---

**Reason for Policy**

This policy provides the University of Oregon’s approach for classifying data and information systems (“information assets”) according to their potential level of risk to the University. The policy and associated procedures also assign roles and responsibilities for protecting information assets and detail how such assets must be protected based on their classifications.

---

**Entities Affected by this Policy**

All users of University of Oregon information.

---

**Web Site Address for this Policy**

(To be updated upon posting)

---

**Responsible Office**

For questions about this policy, please contact the Information Security Office at 541-346-5837 or [infosec@uoregon.edu](mailto:infosec@uoregon.edu)

---

**Enactment & Revision History**

Enacted as a permanent policy by President Schill on April 25, 2016.  
Extended by President Michael Schill on December 15, 2015.  
Enacted as an emergency policy by Dr. Scott Coltrane, Interim President on June 25, 2015.  
This policy supersedes Fiscal Policy Manual 56.350.200-230 and UO Policy 10.00.01.

---

**Policy****Summary**

The purpose of this policy is to outline the acceptable approach for classifying university information assets into risk levels to facilitate determination of access authorization and appropriate security control. The requirement to safeguard information assets must be balanced with the need to support the pursuit of university 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.

## Definitions

**Data Availability** refers to methods for ensuring that required data is always accessible when needed, in accordance with University retention policy.

**Data Confidentiality** refers to methods for ensuring that access to sensitive data is limited to authorized individuals.

**Data Integrity** refers to methods for ensuring that data is complete, accurate, consistent, and safeguarded from unauthorized modification.

**University Data** refers to data owned by or in the legal custody of the University, regardless of source. Personally-owned data stored on University devices is not ~~considered~~ University Data.

## Roles and Responsibilities

### Chief Information Security Officer

The Chief Information Security Officer develops and implements policies and procedures to secure University information assets and comply with state, federal, and international laws and regulations applicable to the University of Oregon.

### Data Trustee

The Data Trustee for all University Data is the Provost or their designees who have planning, policy-level, and management responsibility for data within their designated functional area(s). Data Trustees' responsibilities include:

- Assigning and overseeing Data Stewards.
- Overseeing the establishment of UO information asset policies.
- Determining statutory, regulatory and other University requirements for UO information assets.
- Promoting data quality and integrity and appropriate use.

### Data Stewards

Data Stewards are persons ~~University members~~ having direct operational-level responsibility for the management of one or more types of University data. Data Stewards must be authorized by the appropriate Data Trustee. Data stewards include, but is not limited to, associate deans, associate vice presidents or associate vice provosts, directors, heads of departments, research principal investigators or principal researchers for data they create or receive within the scope of work of their research project, instructors or students for data they create or receive within the scope of a work of their course of program. Data Stewards' responsibilities include:

- Assigning and overseeing Data Custodians.

- Assigning data classification levels in accordance with this policy and associated procedures.
- Collaborating with the CISO in identifying and implementing appropriate administrative and technical safeguards outlined in the UO Minimum Information Security Controls Standard, for protecting information assets (see Related Resources, below).
- Collaborating with the CISO in communicating and providing education on the required safeguards for data to authorized users and Data Custodians.
- Authorizing access, both logical and physical, only to authorized individuals who have a business need – as defined by law and university policies - to access specific data or other information assets.
- Authorizing remote access to information assets to only authorized individuals who have a business need – as defined by law and university policies - to access through a secured system approved by the Chief Information Security Officer.

In cases where multiple Data Stewards collect and maintain the same data elements, the Data Stewards must work together, in collaboration with the CISO, to apply the UO Minimum Information Security Controls.

#### **Data Custodians**

Data Custodians are University personnel or designated third-party agents responsible for the operation and management of information systems which collect, manage, process, or provide access to University Data. Data Custodians must be authorized by the appropriate Data Stewards following procedures outlined in the UO Minimum Information Security Controls Standard (see Related Resources, below). Data Custodians' responsibilities include:

- Applying the UO Minimum Information Security Controls appropriate to the classification level of the data and other information assets in their custody.
- Complying with applicable University acceptable use and computer security policies, standards, and procedures.
- The application of this and related policies and procedures to the systems, data, and other information resources under their care or control.
- Managing Data Consumer access as authorized by appropriate Data Stewards.
- Following data handling and protection policies and procedures established by Data Stewards and the CISO.

#### **Data Consumers**

Data Consumers are the individual University community members or third-party agents who have been granted access to University Data (wherever it is stored) in order to perform assigned duties or in fulfillment of assigned roles or functions for the University. This access is granted solely for legitimate University purposes. Data Consumers' responsibilities include:

- Following the policies and procedures established by the appropriate Data Stewards, Data Custodians, and the CISO.



- Complying with University policies and federal, international, and state laws and regulations associated with the University Data and information system use.
- Implementing safeguards for protecting data as prescribed by appropriate Data Stewards and the CISO.
- Reporting any unauthorized access or data misuse to the Information Security Office, the appropriate Data Trustee, Steward, or Custodian, for remediation.

A current list of UO Data Trustees, Data Stewards, and Data Custodians is available in the UO Data Security Classification Table (see Related Resources, below).

### **Data Classification**

Data Stewards must classify all University data – digital or printed - into risk levels to provide the basis for understanding and applying the appropriate level of security controls. These classification levels consider the state and federal legal protections, contractual agreements, ethical considerations, or strategic or proprietary worth. Data can also be classified as a result of the application of “prudent stewardship,” where the reason to protect the data is to reduce the possibility of harm to individuals or to the institution.

### **Data Classification Levels**

The classification level assigned to data will guide Data Trustees, Data Stewards, Data Custodians, functional and technical project teams, and any others who may create, obtain, process, transmit or store data, in the security protections and access authorization mechanisms appropriate for that data. Data Stewards must classify University Data as one of the following risk levels:

- **Low Risk (or Green)** Data is classified as Low Risk if the loss of confidentiality, integrity, or availability of the data would have *minimal* strategic, compliance, operational, financial, or reputational risk to the University. The integrity of Low Risk data is of primary importance and must be protected. The appropriate Data Trustee or Steward must authorize external release of Low Risk data. Data already released in the public domain by University approved parties is considered “public data” and does not require further authorization for release. Refer to the UO Data Security Classification Table (see Related Resources, below) for examples of Low Risk data.
- **Moderate Risk (or Amber)** Data is classified as Moderate Risk if the loss of confidentiality, integrity, or availability of the data would have *moderate* strategic, compliance, operational, financial, or reputational risk to the University. Integrity and availability of Moderate Risk data are of primary importance and must be protected; privacy and confidentiality should be protected as appropriate. Access to Moderate Risk data must be authorized by the Data Trustee or Steward who is responsible for the data, as needed. Data access authorization may be provided to individuals as part of their job

roles or responsibilities. Refer to the Data Security Classification Table (see Related Resources, below) for examples of Moderate Risk data.

- **High Risk (or Red)** Data is classified as High Risk (the most sensitive/critical classification) if the loss of confidentiality, integrity, or availability of the data would have *high* strategic, compliance, operational, financial, or reputational risk to the University. Privacy, confidentiality, integrity, and availability are important and must be protected. Access to High Risk data must be controlled from creation to destruction, and shall 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 state or federal law. The confidentiality of data is of primary importance, although the integrity of the data must also be ensured. Access to High Risk data must be requested from, and authorized by, the Data Trustee or Steward who is responsible for the data.

High Risk data includes information protected by law. Note: some data that is not regulated may be classified as High Risk by the Data Trustees or Stewards due to proprietary, ethical, or privacy considerations. Refer to the Data Security Classification Table (see Related Resources, below) for examples of High Risk data.

### **Classification of Information Systems and Technology Components**

Information systems and technology components, including computing and storage devices, mobile devices, network components, and applications, adopt the highest classification of the data that they process, store, or transmit. For example, a system that processes, stores, or transmits High Risk data is classified as a High Risk system; whereas a system that processes Moderate Risk data as the highest data classification level is classified as a Moderate Risk system.

In addition to data-specific risks, information systems components may also affect the safety of the UO community, through interference with operational technology (OT) such as building and industrial automated control systems and automation and supervisory control and data acquisition (SCADA) systems. An information system component is also classified as High, Moderate, or Low Risk if unauthorized access or modification or the loss of availability would have a high, moderate, or low safety risk respectively, to the UO community.

### **Data Security Requirements for the Classification Levels**

The Chief Information Security Officer shall create and maintain security procedures for the various types of data use by the University. These requirements are outlined in the UO Minimum Information Security Controls standard (see Related Resources, below). In addition, the CISO will create and maintain additional guidelines and procedures for appropriate handling of data including the [Minimum Security Procedure for Handling Physical University Data \(see Related Resources, below\)](#).

**Related Resources**

[UO Minimum Information Security Controls](#)

[UO Data Security Classification Table](#)

[Minimum Security Procedure for Handling Physical University Data](#)

# Data Security Framework (DSF)

## Overview

The DSF will facilitate classification and protection of University data and systems based on associated SCORF risks (strategic, compliance, operational, reputation or financial risk) to the institution. Understanding the risk levels of different types of data is required for prioritizing investments in cybersecurity and ensuring equitable protection of data and systems. Following are key artifacts included in the DSF:

**Policy - Information Asset Classification and Management Policy (IACMP).** The current [Data Classification Policy](#) is being expanded to become the IACMP. The IACMP expands the classification criteria from focusing on data confidentiality (sensitivity) to also include data integrity and availability. This provides better alignment with university needs and industry best practices to protect data confidentiality, integrity and availability (CIA). The IACMP also includes classification of devices that process, store or transmit data. It simplifies the current classification policy by reducing the number of levels from 4 to 3 – “Public, Internal, Sensitive-Regulated, Sensitive-Unregulated” to “Low Risk (green), Moderate Risk (amber), and High Risk (red). Finally, the policy expands the responsibilities of data stewards accountable for ensuring security of university data and compliance with legal requirements. The redlined version of the policy is attached.

**Standard – Data Security Classification Table.** This table will be published online. It provides a listing of the most common data types, descriptions, examples of data elements, associated classifications, and responsible data stewards and custodians. See sample Data Security Classification Table snippet below.

**Standard – Minimum Security Controls for Protecting Data and Systems by Classifications.** These standards are currently being developed by the Information Security Office in collaboration with university IT staff, data stewards and custodians. They will provide administrative and technical requirements for protecting university data and systems wherever they reside. See sample standard below.

## Process

The updated policy is currently under review by the Information Security Office in collaboration with data stewards and custodians across campus. It will be submitted for approval by the PAC during the May 1<sup>st</sup> session. The approved policy will be published along with the standards mentioned above, then a major training effort will be undertaken as part of the implementation of this policy. Finally, about 18 months after the policy is implemented, the Information Security Office in collaboration with the data stewards will develop and implement a formal program for monitoring compliance with the policy and associated standards.

## Standard - Data Security Classification Table (sample rows)

Data Type	Description & Examples	Security Classification	Office of Record / Steward	Data Steward	Data Custodian
<b>Attorney-Client Privileged and/or Attorney Work-Product Information</b>	<p>Office of General Counsel’s notes, communications and other records maintained related to client and an attorney. Examples of this type of record include:</p> <ul style="list-style-type: none"> <li>Office of General Counsel communications with client that provide legal advice, discuss actual or potential lawsuits, grievances, disputes with third-party vendors, legal holds, subpoenas and requests for information, communication to/from government agencies, etc.</li> <li>Data relevant to the above matters.</li> </ul>	<b>High Risk (Red)</b>	Office of General Counsel	Vice President & General Counsel	Lead IT Service provider for Office of Record
<b>Law Enforcement Information (LEI)</b>	<p>Non-public law enforcement records generated or maintained by the University of Oregon Police Department (UOPD) and Regional Partners (City of Eugene PD, City of Springfield PD, Junction City PD). Examples of this type of information include:</p> <ul style="list-style-type: none"> <li>Unpublished criminal records (NCIC returns, local CHRI)</li> <li>Active investigation information (Case Files)</li> <li>Vehicle/Officer location information (via CAD or GPS)</li> <li>Video recording of police activity (Body Cam, In-car video, Taser video)</li> </ul>	<b>High (Red)</b>	UOPD	UO Police Chief	Lead IT Service provider for Office of Record

	<ul style="list-style-type: none"> <li>• Audio Recording of police activity</li> <li>• Background Check Information</li> <li>• Electronic Fingerprint combined with PII</li> </ul>				
<b>Personally Identifiable Information (PII)</b>	<p>Personally Identifiable Information (PII) is defined as any data element or combination of data elements that would be sufficient to be used to fraudulently assume the identity of an individual. Examples of this type data include a person's <b>name</b> in combination with one or more of the following:</p> <ul style="list-style-type: none"> <li>• Social Security number (note: UOIDs or 95#s are treated as <i>Moderate</i>)</li> <li>• W2s, W4s, I9s</li> <li>• Driver's license number or state identification card number</li> <li>• Identification number issued by a foreign nation</li> <li>• Passport number</li> <li>• Bank Account number, Credit Card number or Debit Card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account</li> <li>• Biometrics</li> <li>• Date of Birth</li> </ul>	High (Red)	<p>University Registrar's Office</p> <p>Law School</p> <p>Human Resource Office</p> <p>University Libraries</p> <p>University Advancement</p> <p>Business Affairs Office (BAO)</p> <p>Office, Department or Lab that Received the Data</p>	<p>University Registrar</p> <p>Law School Registrar</p> <p>Chief Human Resource Officer</p> <p>Dean of Libraries</p> <p>Senior Associate Vice President of Development Advancement</p> <p>Associate Vice President, Business Affairs Office</p> <p>Head of Office, Department or Lab that Received the Data</p>	Lead IT Service providers for Offices of Record

<b>Student Records (non-directory)</b>	Student educational records designated as “nondirectory information” by the University Registrar’s Office. The Family Educational Rights and Privacy Act (FERPA) governs release of, and access to, student education records. Examples of this type of information are listed on the Registrar’s website at: <a href="https://registrar.uoregon.edu/records-privacy">https://registrar.uoregon.edu/records-privacy</a>	Moderate (Amber)	University Registrar’s Office  Law School Registrar’s Office	University Registrar  Law School Registrar	Lead IT Service providers for Offices of Record
<b>Student Records (directory information)</b>	Student educational records designated as “directory information” by the University Registrar’s Office; by default these records can be released without student approval. Students can request nondisclosure by filing a Directory Information Restriction via the Registrar’s Office. Examples of this type of information are listed on the Registrar’s website at: <a href="https://registrar.uoregon.edu/records-privacy">https://registrar.uoregon.edu/records-privacy</a>	Low (Green)	University Registrar’s Office  Law School Registrar’s Office	University Registrar  Law School Registrar	Lead IT Service providers for Offices of Record

## Standard - Minimum Security Controls by Classification (sample section)

Control	Information System Classification M – Mandatory; R – Recommended; NR – Not Required			Applicable Service
	High Risk (Red)	Moderate Risk (Amber)	Low Risk (Green)	
<b>IDENTIFICATION Controls</b>				
UO.ID.1 Configuration Management System (CMS): Registration	M	M	M	SCCM, JAMF, Puppet
<b>PROTECTION Controls</b>				
UO.PR.1 Physical Security	M	R	NR	Datacenter, O365, ...
UO.PR.3 System Hardening	M	M	R	
UO.PR.7 Anti-malware	M	M	M	McAfee
UO.PR.10 Firewall	M	M	R	
UO.PR.12 Encryption: Data-in-Transit	M	M	R	
UO.PR.20 User Access Control: Two-Factor Authentication	M	R	R	DUO 2FA
<b>DETECTION Controls</b>				
UO.DE.1 Logging and Retention	M	R	NR	
UO.DE.2 Log Monitoring	M	R	NR	
<b>RECOVERY Controls</b>				
UO.RE.1 Incident Recovery: Backup & Recovery	M	R	R	
UO.RE.2 Incident Recovery: Restoration Testing	M	R	R	

## Glossary (sample)

UO.PR.1	Physical Security	<p><b><i>System shall be physically protected and monitored to prevent theft or unauthorized access to data via the system consoles or keypads.</i></b></p> <p>System should be hosted within a protected and monitored area with a secure perimeter (e.g., walls, lockable doors and windows) that protects the system from unauthorized physical access. UO datacenters should be used for hosting server devices. Endpoint devices should be kept safe to prevent them becoming loss or stolen.</p>
---------	-------------------	--