UNIVERSITY OF OREGON

Policy Concept Form

As part of the University of Oregon Policy development process, all new Policy proposals, as well as proposals for the revision or repeal of existing Policies, must be submitted via this form to the University Secretary (the policy custodian). The Secretary will forward completed concept forms to the President's Policy Advisory Council for consideration pursuant to the University's Policy on University Policies. Please remember:

> A "Policy" as defined by the University Policy on Policies (1) has broad application or impact throughout the University community, (2) must be implemented to ensure compliance with state or federal law, (3) is necessary to enhance the University's mission, to ensure institutional consistency and operational efficiency, or to mitigate institutional risks; or (4) is otherwise designated by the Board or the President as a University Policy subject to the Policy-Making Process authorized in section **Error! Reference source not found.**. A policy establishes rights, requirements or responsibilities. Excluded from this definition are things such as, but not limited to, implementation guides, operating guidelines, internal procedures, and similar management controls and tools.

[Complete the following information as thoroughly as possible; response boxes will expand as filled.]

CONCEPT SUBMITTED BY:

NAME:	Will Laney
PHONE:	541-346-9700
EMAIL:	wlaney@uoregon.edu
ORGANIZATION:	UO Information Security Office (a unit of Information Services)

POLICY CONCEPT SUBJECT MATTER (including existing policy number if appropriate):

The University of Oregon Data Classification Policy

STATEMENT OF NEED FOR THIS POLICY CONCEPT (i.e. What is the problem this concept seeks to address, and how does this proposal do so?):

The University needs a formal data classification policy in order to determine which data we need to better protect. We have also developed procedures that specify ways to protect the data

WHO OR WHAT MIGHT BE AFFECTED BY THIS POLICY CONCEPT, AND HOW? ***List all individuals, groups, etc. that would be impacted by this concept and the nature of any possible impacts (both positive and negative).***

This policy will affect most members of the University community. Individuals will need to classify their data and apply security to data that is more sensitive in nature.

WHAT COSTS MIGHT BE ASSOCIATED WITH THIS CONCEPT, BOTH IMPLEMENTATION AND RECURRING?

Costs would include time to classify data and time to set security settings on computer systems.

WHAT OTHER RESOURCES (HUMAN, PHYSICAL, OPERATIONAL, FINANCIAL, TECHNOLOGICAL, ETC.), WILL BE NEEDED TO IMPLEMENT AND MAINTAIN COMPLIANCE WITH THIS POLICY?

Human resources will be needed to classify and secure the data. The recommended security practices are written so that they should not require additional hardware or software.

DOES THE PROPOSED CONCEPT IMPACT EXISTING POLICIES, GUIDELINES OR PROCEDURES? DOES THE PROPOSED CONCEPT RELATE TO A MATTER WITHIN A UNION CONTRACT? IF SO, PLEASE LIST.

This policy will replace part of OUS Information Security Section: General Operations Number: 56.350. (specifically 200-230)

ADDITIONAL INFORMATION YOU WISH TO SHARE?

PLEASE PROVIDE ANY SUGGESTED LANGUAGE AS AN ATTACHMENT TO THIS FORM.

FOR OFFICE USE ONLY

Date Received:

Why is there a need to have these as emergency policies?

(a) Practical Need

Information Security policies are the cornerstone of an Information Security Program. The Chief Information Security Officer (a new position at UO) is requesting that these policies be implemented as emergency policies because UO has very few information security policies and those it does have are lacking compared to policies at peer and inspirational institutions. The lack of a Data Classification policy holds up decisions about the types of data we own and where it can be stored. For example, while many people use the term "sensitive data" there has never been a true definition of what types of data are sensitive. This document will resolve that issue. As another example, the lack of a Data Security Incident Response policy leads to situations where the response to security incidents can vary greatly across campus. By centralizing the response we can apply consistent and repeatable practices to our security incidents.

Commented [BD1]: I would provide more detail as to why they are lacking, particularly with respect to technologies. I might also think of additional examples you could use in this paragraph.

(b) Legal/Regulatory Need

These policies are required by Oregon law. Oregon's Consumer Identity Theft Protection Act, ORS 646A.600 to 646A.628 (CITPA), requires any entity that owns, maintains, or otherwise possesses data that includes a consumer's personal information to develop, implement, and maintain safeguards, standards, and programs to protect, among other things, the security and integrity of such information. Such policies are also specifically dictated by OUS Information Security Policy (OAR 580-055-0000), which is required to "be used by each OUS institutions' management to develop, document, implement, and maintain local information security policy and programs." Furthermore, data security and breach notification policies are required by other federal statutory and regulatory schemes that govern certain pieces of this area—e.g., the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing rules and regulations, and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") of the American Recovery and Reinvestment Act of 2009 ("ARRA")

And while FERPA does not contain specific requirements relating to data breach, the Department of Education, as the federal agency that enforces FERPA, recently concluded that every educational institution "should create a data breach response policy, approved by the organization's leadership, that is germane to its environment."

A number of statutes and regulations that UO must follow (such as CITPA, FERPA, HIPAA) and security standards that it should follow (such as PCI) require various security policies to be in place. This first round of policies will greatly improve our compliance position.

Who have reviewed these policies?

These policies have been vetted with the Library, Research, and the following IT Advisory Groups: Campus Technology Council, Services and Operations Advisory Group, Educational Technology Advisory Group, IT Directors Advisory Group, Banner Coordinating Group, and Research Cyberinfrastructure Advisory Group. The policies have also been reviewed by the Policy Advisory Council (PAC).

Are these policies in reaction to the release of the 20,000 documents in the Presidents' personal correspondence?

No. The decision was made to wait until a Chief Information Security Officer (CISO) was hired to write the policies. The new CISO was hired into that position in November of last year and started working on these policies. They were developed before the incident with the letters occurred.

Are there any issues related to Academic Freedom?

During a meeting with the PAC, the University Senate wanted to review and provide input to these policies. The CISO will work with the University Senate to address and amend the policies during the Fall Semester. Emergency policies will expire in six months and once we have input from the University Senate we will again go through the PAC process. In the meantime, we feel that these Information Security policies are required, and that campus needs such policies to guide them in better security University data, computers, and networks.

Are there any issues related to Research?

Yes. A number of research granting organizations (especially Government-based) are beginning to require security policies. These policies will help our Researchers remain competitive in their applications for research grants.

How do these policies relate to OUS policies?

As UO has moved away from OUS, we are attempting to replace and greatly enhance the OUS policies with definitive UO policies. These three policies will allow for some older OUS polices to be removed from the policy library.

Will these policies have an effect on the current Collective Bargaining negotiations?

These policies should not affect any of the current Collective Bargaining negotiations. While there are issues related to computer appropriate use in the Collective Bargaining process, we do not believe that the Information Security policies will preclude or conflict with the acceptable use conditions.

UNIVERSITY OF OREGON

POLICY IV.06.XX
Data Classification

REASON FOR POLICY

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

UO Faculty, Staff, Students, Vendors, Contractors, and any other person allowed access to UO information assets.

WEB SITE ADDRESS FOR THIS POLICY

http://policies.uoregon.edu/sites/policies.uoregon.edu/files/uploads/Data%20Classification%20Policy_0.pdf

---

RESPONSIBLE OFFICE

For questions about this policy, please contact the Chief Information Security Officer at 541-346-9700 or wlaney@uoregon.edu.

ENACTMENT & REVISION HISTORY

Enacted as an emergency policy by Dr. Scott Coltrane, Interim President on June 25, 2015. This policy supersedes OUS Fiscal Policy Manual 56.350.200-230 and UO Policy 10.00.01. OUS Information Security

---

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 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 there is no reason to protect the data other than 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)**
  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 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.

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 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 state and federal laws and regulations 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 Stewards
- Overseeing the establishment of data policies in their areas
- Determining statutory and regulatory requirements for data in their areas
- Promoting appropriate use and data quality

Data Stewards

Data Stewards are University officials having direct operational-level responsibility for the management of one or more types of data. Data Stewards are assigned by the Data Trustee and are generally associate deans, associate vice presidents, directors or managers. Data Steward 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
- Authorize access, both logical and physical, only to Authorized Personnel who have a business need to access specific data or other information assets

- Authorize remote access to information assets to only Authorized Personnel who have a business need 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 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 Stewards. 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 Stewards
- Following data handling and protection policies and procedures established by Data Stewards 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 Stewards and Information Security
- Complying with federal and state laws and regulations, and University policies associated with the University data used
- Implementing safeguards prescribed by appropriate Data Stewards for Sensitive Data
- Reporting any unauthorized access or data misuse to Information Security as well as the appropriate Data Trustee, Steward, and Custodian, for remediation

---

RELATED RESOURCES

University of Oregon Data Classification Procedures:

http://policies.uoregon.edu/sites/policies.uoregon.edu/files/uploads/Minimum%20Security%20Procedure%20for%20Devices%20with%20Sensitive%20Information.pdf

http://policies.uoregon.edu/sites/policies.uoregon.edu/files/uploads/Minimum%20Security%20Procedure%20for%20Devices%20with%20Public%20or%20Internal%20Information.pdf

http://policies.uoregon.edu/sites/policies.uoregon.edu/files/uploads/Minimum%20Security%20Procedure%20for%20Handling%20Physical%20University%20Data.pdf

Detailed below:

Minimum Security Procedure for Devices with Sensitive Information

Summary

This document outlines the minimum security procedures that are required for devices that store or process sensitive University data. The purpose of these requirements is to reduce risks to the confidentiality and integrity of sensitive University data (detailed in **The University of Oregon Data Classification Policy**) and to protect the privacy of members of the University community.

Scope

This standard applies to all devices that store or process sensitive University data, including privately owned devices. Examples of these devices include servers, workstations, laptop computers, tablets, smart phones, printers, etc.

Standard

All devices that store or process sensitive data shall meet the following minimum security requirements.

Servers:

Physical security — Server class devices shall be placed 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.

Security updates — Devices shall be kept up-to-date with current operating system and third-party applications security patches and updates.

Anti-virus software — Anti-virus software shall be used and kept up-to-date if such software is available for the device.

Software firewall — Firewall software shall be used and kept up-to-date.

Limit network access — Network access to sensitive systems shall be restricted to the least access necessary for the device to perform its function/mission.

Access control — User accounts and users shall have a unique identifier (user ID/login name) that is assigned for their University business use only. Privileges shall be restricted and controlled in accordance with the principle of least privilege to reduce opportunities for unauthorized access or misuse of the system. Access and privileges shall be authorized by an appropriate authority and reviewed at regular intervals.

Secure login and authentication — Access shall be controlled with secure/encrypted log-on procedures.

Protection against brute force login attacks — Controls shall be put in place to limit failed login attempts.

Session controls — Controls shall be put in place to ensure that inactive sessions shall expire after a defined period of inactivity.

Logging and monitoring — System administrator and user activities and system events shall be logged. Logs shall be retained for a period of at least one year or a period deemed practicable by the University department/unit responsible for the security of the device, consistent with any applicable retention requirement.

Identification and management of vulnerabilities — Devices shall be hardened prior to implementation. Security updates shall be applied and unnecessary services disabled in order to minimize potential technical vulnerabilities.

Responsibility for security — Responsibility for the security of a sensitive server and its data shall be assigned to an individual.

Encrypted transmission of data — Encrypted protocols or secure channels shall be used to transmit sensitive data to and from the device.
Encrypted storage of data — Sensitive data should be stored in an encrypted state or have compensating controls to secure the data.

Desktops:
Physical security — Desktop devices shall be placed in reasonably secure areas such as lockable offices and not in publically assessable areas.
Login and authentication — Login or authentication procedures shall be used to prevent unauthorized logical access to devices.
Automatic security updates — Desktop devices shall be configured to automatically download and install security updates for operating systems and third-party applications whenever possible.
Anti-virus software — Anti-virus software shall be used and kept up-to-date.
Software firewall — Firewall software shall be used and kept up-to-date.
Auto-lock screens — Desktop devices shall be configured to automatically lock and require a logon after being unattended or inactive for a predefined period of time.
Least privilege for user accounts — User accounts shall be configured with the least privileges necessary for the users to perform their job/role.
Remove sensitive data when no longer needed — Devices shall be configured to automatically delete temporary files, temporary internet files, clear web browser caches, etc.
A process shall be adopted to regularly review archived files and delete files containing sensitive data when the files are no longer needed, consistent with applicable retention laws and regulations, or University policies.

Laptops, tablets, and mobile devices:
Physical security — Laptops (and where available/appropriate tablets and mobile devices) shall be protected from unauthorized physical access and theft by storing the device in a secure location, anchoring with a security cable, etc.
Login and authentication — Login or authentication procedures shall be used to prevent unauthorized logical access to devices.
Automatic security updates — Devices shall be configured to automatically download and install security updates for operating systems and third-party applications whenever possible.
Anti-virus software — Anti-virus software shall be used and kept up-to-date if such software is available for the device.
Software firewall — Firewall software shall be used and kept up-to-date if such software is available for the device.
Auto-lock — Devices shall be configured to automatically lock and require a logon, pin, or other means of authentication after being unattended or inactive for a predefined period of time.
Least privilege for user accounts — User accounts shall be configured with the least privileges necessary for the users to perform their job/role.

Review of Procedure
This Procedure will be reviewed on an annual basis to implement, change, or remove controls based on altered security specifications and changes in statutes, regulations, and best practices.

Minimum Security Procedure for Devices with Public or Internal Information

Summary
This document outlines the minimum security procedures that are required for devices that store or process public or internal University data. The purpose of these requirements is to reduce risks to the confidentiality and integrity of public or internal University data (detailed in **The University of Oregon Data Classification Policy**) and to protect the privacy of members of the University community.

Scope
This standard applies to all devices that store or process public or internal University data, including privately owned devices. Examples of these devices include laptop computers, tablets, smart phones, printers, etc.

Standard
All devices that store or process public or internal data shall meet the following minimum security requirements.

Security updates
Devices shall have all applicable security updates for operating systems and third-party applications installed as soon as practicable or, at a minimum, within 2 weeks of the security update release date.

Anti-virus software
Anti-virus software shall be used and kept up-to-date on devices where the use of such software is practical.

Software firewall
Firewall software shall be used and kept up-to-date on devices that have firewall software capabilities.

Access control
Devices shall require sign-on or login for users. Users shall be authenticated by means of passwords or by other authentication processes (e.g., biometrics or Smart Cards). In general, only encrypted authentication mechanisms or protocols shall be used.

Unnecessary services
Services that are not necessary for the device to perform its function or mission shall be disabled.

Review of Procedure
This Procedure will be reviewed on an annual basis to implement, change, or remove controls based on altered security specifications and changes in statutes, regulations, and best practices.

Minimum Security Procedure for Handling Physical University Data

Summary
This document outlines the minimum security standards that are required for individuals who handle physical data (such as printed reports, letters, or memos) containing sensitive or internal University data. The purpose of these requirements is to reduce risks to the confidentiality and integrity of

sensitive or internal University data (detailed in The University of Oregon Data Classification Policy) and to protect the privacy of members of the University community.

Scope
This standard applies to all individuals who handle physical data containing sensitive or internal University data.

Standard
Granting Access or Sharing
Access shall be limited to authorized University officials or agents with a legitimate educational or business interest on a need to know basis.

Storage
If data needs to be retained while not being used or reviewed, the data must be stored in a locked device (such as a filing cabinet) and also be protected by a locked door when staff are not present.

Disclosure, Public Posting, etc.
Reasonable methods shall be used to ensure data is only disclosed to authorized individuals or individuals with a legitimate need to know. Sensitive and internal data may not be posted publicly.

Printing, mailing, fax, etc.
Reasonable methods shall be used to ensure that printed materials are only distributed or available to authorized individuals or individuals with a legitimate need to know. Printed materials that include sensitive data shall only be distributed or available to authorized individuals or individuals with a legitimate need to know. Access to any area where printed records with sensitive and internal data are stored shall be limited by the use of controls (e.g. locks, doors, monitoring, etc.) sufficient to prevent unauthorized entry.

Disposal
When the data is no longer needed, and no longer required to be retained per records retention requirements, the paper should be shredded with a cross-cut shredder or destroyed by another appropriate method (such as a secured burn/destruction box).

Review of Procedure
This Procedure will be reviewed on an annual basis to implement, change, or remove controls based on altered security specifications and changes in statutes, regulations, and best practices.