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):

UO Data Security Incident Response 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?):

This policy will create a standard way for information security incidents to be reported and handled.

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 allow all members of the University community a way to notify Security Professionals of potential security incidents.

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

Cost will be minimal as this service is already provided. It is a formalization of current practices.

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 and they are currently used in response to security incidents.

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 240)

ADDITIONAL INFORMATION YOU WISH TO SHARE?

This policy is used to point to the procedures where the real detail is located. This was done so that we can refine the process over time without having to go through a formal policy review

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 Security Incident Response

REASON FOR POLICY

This policy will provide for a consistent and repeatable process for responding to data security incidents.

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/UO%20Data%20Security%20Incident%20Response%20Procedure.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 56.350.240 Incident Response.

POLICY

The University of Oregon is committed to compliance with all applicable state and federal and laws and regulations relating to the compromise of Sensitive Data (as detailed in the University of Oregon Data Classification Policy). In the event that paper or electronic records containing sensitive data are subject to an unauthorized release or access to unauthorized persons, *The University of Oregon Data Security Incident Response Procedure* must be used to determine whether any sensitive data have in fact been exposed, what specific data were exposed, the impact of the exposure, and what actions are required for legal compliance related to the exposure.

Scope: Any University of Oregon faculty, staff, student, vendor or contractor who believes that sensitive data has been potentially exposed to unauthorized persons must immediately notify the UO Information

Security Office. Individuals can either send an email to security@ithelp.uoregon.edu or call (541) 346-5837.

RELATED RESOURCES

University of Oregon Data Security Incident Response Procedures:
http://policies.uoregon.edu/sites/policies.uoregon.edu/files/uploads/UO%20Data%20Security%20Incident%20Response%20Procedure_0.pdf

Detailed below:

The University of Oregon Data Security Incident Response Procedure

Data security incident reporting responsibility: Any University of Oregon faculty, staff, student, vendor or contractor who believes that sensitive data (as detailed in the University of Oregon Data Classification Policy) was or may have been exposed to unauthorized persons must immediately notify the UO Information Security Office. Individuals can either send an email to security@ithelp.uoregon.edu or call (541) 346-5837.

Data security can be compromised in a variety of ways. The following is a list of common (but not exclusive) ways data can be breached:

- Malware infection or system vulnerability allowing unauthorized access into the system or unauthorized retrieval of data from a system
- Unintended disclosure on a public or internal website or through physical or electronic mail
- Payment card fraud involving skimming devices at point of sale terminals
- Lost or stolen paper documents or computing equipment/device (laptop, PC, smartphone, tablet, or backup media)

In the event that paper or electronic records containing sensitive data were or may have been exposed to unauthorized persons, the following protocols shall be executed.

Affected Unit Responsibilities (electronic records):

1. Immediately contain and limit the exposure of data. Isolate compromised systems from the network (e.g., unplug the cable). Preserve electronic evidence. Do not shut down, reboot, access or otherwise alter the machine.
2. Alert the UO Information Security Office by sending an email to security@ithelp.uoregon.edu or calling (541) 346-5837.
3. Conduct a thorough investigation of the suspected exposure and maintain a log of all actions taken. This must be coordinated with the UO Information Security Office.
4. Determine root cause in consultation with the UO Information Security Office. Examples include: forensics on cloned hard drive, system log review, and analysis of systems running in memory.

5. Determine data exfiltration in consultation with the UO Information Security Office. Network and system log review.
6. Work with the UO Information Security Office to draft a Security Incident Report identifying all information at risk and the source and timeframe of the compromise. Share this report with the Data Security Incident Response Team (DSIRT).
7. Notify affected customers if directed by the DSIRT, in consultation with the Office of the General Counsel (OGC).
8. Remediate as directed by the DSIRT.

Affected Unit Responsibilities (paper based or lost computing equipment):

1. Alert the UO Information Security Office by sending an email to security@ithelp.uoregon.edu or calling (541) 346-5837.
2. Determine the type and volume of data potentially exposed.
3. For paper based breaches, determine when and where the paper was lost and/or exposed.
4. For lost computing equipment, determine if there is the ability to remotely wipe the data storage on the device. Determine if the device was password protected and if data was encrypted.
5. Work with the UO Information Security Office to draft a Security Incident Report identifying all information at risk and the source and timeframe of the compromise. Share this report with the Data Security Incident Response Team (DSIRT).
6. Notify affected customers if directed by the DSIRT.
7. Remediate as directed by the DSIRT.

Data Security Incident Response Team (DSIRT): The entire team consists of the Chief Information Security Officer, Office of the General Counsel, University Registrar, HIPAA Compliance Officer, Chief Human Resources Officer, AVP for Business Affairs, Media Relations, Chief Auditor, and UO Police Department.

When responding to a particular security incident, the core of the Team will be the Chief Information Security Officer, Office of the General Counsel, and Data Steward of the particular type of data that is involved. The Dean/Director of the affected unit will also be involved in the process. Other Team members will be added as needed.

This Team, in consultation with the Office of the General Counsel, will review the Security Incident Report and determine whether a Data Breach occurred, and whether or not the following actions are warranted under applicable law

a) Notify local law enforcement or any state or federal governmental entity (e.g., FBI);
b) Notify affected customers
c) Notify other third parties for breaches involving: credit cards, education records, health records, research subject data, donor information, or other records.

The Data Security Incident Response Team will evaluate and evolve the data security incident response procedure based on lessons learned in responding to potential breaches, and work to establish the steps necessary to prevent or limit the risk of the incident recurring.

Notice Requirements

The method and timing of noticing a Data Breach varies depending on the number of individuals affected, the type of information accessed or acquired, the cost of noticing, the legitimate needs of law enforcement agencies, and the normal means of communication with affected individuals, but in all instances as guided by the applicable state or federal law.

Responsibility

Financial costs incurred to mitigate a data breach, (such as fines, penalties, investigations, litigation, communications, credit monitoring etc.), will be borne by the college or administrative unit deemed responsible for the exposure by the DSIRT.

Reference

The following chart details the Data Stewards for the most common types of data on campus:

Records	Steward
Student education records	University Registrar
Employee records	Chief Human Resources Officer
Credit card or bank account data	AVP Business Affairs
Personal health information	HIPAA Compliance Officer
Human Subject Data	Research Compliance Services

Data Security Incident Response

Policy Number:
IV.06.03

Reason for Policy:

This policy will provide for a consistent and repeatable process for responding to data security incidents.

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 56.350.240 Incident Response.

Policy:

The University of Oregon is committed to compliance with all applicable state and federal and laws and regulations relating to the compromise of Sensitive Data (as detailed in the University of Oregon Data Classification Policy).

Data Exposure Investigation: In the event that paper or electronic records containing sensitive data are subject to an unauthorized release or access to unauthorized persons, *The University of Oregon Data Security Incident Response Procedure* must be used to determine whether any sensitive data have in fact been exposed, what specific data were exposed, the impact of the exposure, and what actions are required for legal compliance related to the exposure.

Notification: The decision on notification will be made by the Office of the General Counsel based on applicable Federal and State law.

Security Incident Reports Annual Summary: On an annual basis a summary of Security Incident Reports will be produced by the CISO that will detail the number of Reports issued and how many of the Reports required notification (upon the decision of the Office of the General Counsel). Given the nature of these investigations, these summary reports cannot risk further exposure of sensitive information, and so can be expected to be minimal in their level of detail beyond the two requirements stipulated herein (namely, a summary accounting of the number of Reports issued and how many of the Reports required notification).

Scope of Duty to Report: Any University of Oregon faculty, staff, student, vendor or contractor who has a reasonable cause to believe that sensitive data has been exposed to unauthorized persons must immediately notify the UO Information Security Office. Individuals can either send an email to security@ithelp.uoregon.edu or call (541) 346-5837. Employees who identify themselves and make a good faith report of suspected fraud, waste, or abuse are protected from retaliation, in accordance with Oregon law. UO will maintain confidentiality for employees reporting suspected irregularities, misconduct, safety issues, or other concerns to the extent possible under the law.

Data Security Incident Response

Policy Number:
IV.06.03

Reason for Policy:

This policy will provide for a consistent and repeatable process for responding to data security incidents.

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 56.350.240 Incident Response.

Policy:

The University of Oregon is committed to compliance with all applicable state and federal and laws and regulations relating to the compromise of Sensitive Data (as detailed in the University of Oregon Data Classification Policy).

Data Exposure Investigation: In the event that paper or electronic records containing sensitive data are subject to an unauthorized release or access to unauthorized persons, *The University of Oregon Data Security Incident Response Procedure* must be used to determine whether any sensitive data have in fact been exposed, what specific data were exposed, the impact of the exposure, and what actions are required for legal compliance related to the exposure.

Notification: The decision on notification will be made by the Office of the General Counsel based on applicable Federal and State law.

Security Incident Reports Annual Summary: On an annual basis a summary of Security Incident Reports will be produced by the CISO that will detail the number of Reports issued and how many of the Reports required notification (upon the decision of the Office of the General Counsel). Given the nature of these investigations, these summary reports cannot risk further exposure of sensitive information, and so can be expected to be minimal in their level of detail beyond the two requirements stipulated herein (namely, a summary accounting of the number of Reports issued and how many of the Reports required notification).

Scope of Duty to Report: Any University of Oregon faculty, staff, student, vendor or contractor who has a reasonable cause to believe~~believes~~ that sensitive data has been ~~potentially~~ exposed to unauthorized persons must immediately notify the UO Information Security Office. Individuals can either send an email to security@ithelp.uoregon.edu or call (541) 346-5837. Employees who identify themselves and make a good faith report of suspected fraud, waste, or abuse are protected from retaliation, in accordance with Oregon law. UO will maintain confidentiality for employees reporting suspected irregularities, misconduct, safety issues, or other concerns to the extent possible under the law.