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) or Personally Identifiable Information (PII) have 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.

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 or PII are potentially 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.
7. Notify affected customers if directed by the Data Security Incident Response Team.
8. Remediate as directed the UO Information Security Office.

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.
6. Notify affected customers if directed by the Data Security Incident Response Team.

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

When responding to a particular security incident, the core of the Team will be the Chief Information Security Officer, Office of 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 will review the Security Incident Report and determine whether or not the following actions are warranted:

a) Engage local law enforcement or 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.

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.

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 records	HIPAA Compliance Officer
Human Subject Data	Research Compliance Services