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.