

Incident Response, Notification and Escalation Plans

(OAR 580-055-0050-4A,B)

The purpose of this section is to clarify and formalize security operations and procedures in the event of information security incidents.

The scope of these procedures is limited to information security and where physical security overlaps the appropriate coordination with Campus Security is assumed and will be conducted in accordance with Campus Security established protocols and procedures. Where information security overlaps with personnel action or student confidentiality, the appropriate coordination with Human Resources, the Registrar's Office, and Student Affairs is assumed and will be conducted with established protocols and procedures.

These procedures apply to all information security incidents which involve Institutional Information classified as Protected Information and may be used for incidents involving Institutional Information classified as Sensitive Information depending on the nature of the incident and the asset involved.

In compliance with RFC2142, EOU does maintain an appropriate email aliases for the reporting of various activity originating from hosts on EOU's network. The abuse@eou.edu alias in particular is widely accepted across the internet and specifically identified by EOU in our network registration as the appropriate alias to notify when a breach is suspected. The Network Systems Manager maintains this email alias, responds to and track all reports and incidents and will ask that responsible parties verify whether or not Protected Information or Sensitive Information was involved.

In the case where Protected Information is involved, these incidents will be initially escalated to the Chief Information Security Officer (CISO) or the appropriate Data Steward who will initiate an incident response report in concert with the CISO. Incidents involving Protected Information will be reviewed by the Data Steward and potentially legal counsel to ensure appropriate responses are taken in accordance with Oregon law. As appropriate, a copy of the report will be shared with the University Cabinet. As stated in the scope statement, incidents overlapping with physical security, personnel action, or student conduct will be handled in accordance with established protocols and procedures; however, the CISO will be appraised to ensure that information Security specific aspects of any incident are addressed.

April 3, 2008