Information Security Incident Response Escalation Guideline

Background

Information security incidents vary greatly in their criticality and impact on the business mission of the university. The purpose of this guideline is to define escalation and notification procedures in the event of an information security incident. This guideline is designed to work in conjunction with the Information Security Incident Management and Response Policy, Incident Response Procedure and Data Protection Policy.

Incident Notification

Incident Type	Department Notified
Incidents involving confirmed or potential criminal activity	UCPD
Lost or stolen devices	UCPD Director of Privacy (if data suspected lost) Departmental asset owner
Litigation Hold	Office of General Counsel
Public Records Request	Office of General Counsel Data owner
Faculty/staff email or data request	Office of General Counsel
Student email or data request	Office of General Counsel
Inappropriate content	HR Office of General Counsel Employee Supervisor
EthicsPoint Complaint	Office of Internal Audit Office of General Counsel UCPD (if criminal)
Research misconduct	Office of Research and Compliance
Academic dishonesty	Office of University Judicial Affairs

OEOA Complaint	Office of Equal Opportunity and Access HR Office of General Counsel
Electronic harassment	Title IX Office HR
Compromised system	Asset owner Director of Privacy (if data suspected lost) Emergency Management (in incidents classified as “High” per the Incident Response Procedure)
Compromised account	IT@UC Department IT
Resource misuse	Department head HR Office of General Counsel
HIPAA or FERPA violation	Director of Privacy
Export Controlled data misuse	Export Controls Office
Malware	Department IT

Related Links

Data Governance & Classification Policy
Information Security Incident Management and Response Policy
Information Security Incident Response Procedure

Contact Information

IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu

History

Issued: 1/23/2019