University of Oregon Data Security Incident Response Procedure

Purpose

This procedure outlines steps, roles and responsibilities for effectively addressing cybersecurity incidents to minimize damages and maximize availability of services to support the research and academic mission of the University of Oregon (UO). It outlines expected activities for the full lifecycle of incident response, from planning and preparation to post-incident activities. This procedure provides the steps necessary to comply with the UO Data Security Incident Response Policy and aligns our procedure with best practices.

Key Stakeholders

- **Information Security Office (ISO).** The Information Security Office, under the leadership of the Chief Information Security Officer (CISO), with overall responsibilities for coordinating responses to cybersecurity incidents. The CISO serves as the Incident Commander for cybersecurity incidents.
- **Data Stewards**. Individuals identified as data stewards (by the **University of Oregon Information Asset Classification and Management Policy**) of the systems and data potentially affected by the incident.
- **Data Custodians (or System Owners).** Individuals identified by data stewards as primary custodians of the systems potentially affected by the incident.
- **System Administrators**. IT professionals with operational responsibilities for supporting the systems potentially affected by the incident.
- **Executive Leadership**. University President, Provost and Executive Vice President, Chief Information Officer, Deans, Vice Presidents/Provost or Associate Vice Presidents/Vice Provosts of units where the incident occurred.
- **Incident Management Team (IMT).** Provides the command and control infrastructure that is required to manage the logistical, fiscal, planning, operational, safety, and campus issues related to any and all incidents/emergencies.
- **Sensitive Data**. Includes data classified under the **University of Oregon Information Asset Classification and Management Policy** as High Risk as a result of significant harm to the university if there is a breach. Examples of High Risk data include Protected Health Information (PHI) covered under the Health Insurance Portability and Accountability Act (HIPAA); some Student Educational Records protected under the Family Educational Rights and Privacy Act (FERPA); Controlled Unclassified Information (CUI) protected under federal laws; Personally Identifiable Information (PII) such as social security numbers protected under Gramm-Leach-Bliley Act (GLBA) and Oregon Consumer Identity Protection Act (OCIPA); Credit card data protected under the Payment Card industry Data Security Standard (PCI DSS); Covered data that are protected under the European Union General Data Protection Regulation (GDPR).

Data Security Incident Response Team (DSIRT)

The full DSIRT provide general oversight for the incident response program, and consists of:

- Chief Information Security Officer (Chair)
- Office of the General Counsel representative
- University Registrar
- Chief Human Resources Officer
- AVP for Business Affairs
- External Communication: University Spokesperson; Director of Communications, Safety & Risk Services
- Internal Communication: Strategic Communication Specialist
- University HIPAA and Privacy Officer
- Director of Operations, Safety and Risk Services
- Risk Manager, Safety and Risk Services
- UO Chief of Police
- Chief Auditor

In the event of a specific incident, the core DSIRT response team will be:

- Chief Information Security Officer (Incident Commander)
- Office of the General Counsel
- Chief Auditor
- Data Steward of the affected data
- System owners/system administrators of the affected systems
- Deans/Vice Presidents/Vice Provost or AVPs, and Directors of units where the incident occurred will also be involved in the process.
- Other Team members and subject matter experts will be added as needed.

Phase I – Planning and Preparation

There are two key objectives of the Planning and Preparation phase of the incident response procedure – preparation and prevention.

Preparation

To ensure fast and effective response to incidents, help the UO to minimize damages and maximize service availability, the UO community must perform the following preparatory responsibilities:

- **Report Incidents** - Send an email to the Information Security Office (ISO) at infosec@uoregon.edu or call **(541) 346-5837.** Any UO faculty, staff, student, vendor or contractor who believes that sensitive data (as detailed in the **University of Oregon Information Asset Classification and Management Policy**) may have been exposed to unauthorized persons must immediately notify the ISO.
- **Classify Systems & Data** – All data stewards, custodians, system owners and administrators must classify their systems and data according to the **University of Oregon Information Asset Classification and Management Policy.** Data stewards, system

owners and administrators are expected to know the classification of their systems based on the data they process, store or transmit.

- **Maintain Application System Architecture & Data Flow Diagrams** – All system owners and administrators of systems with High Risk data are expected to maintain up-to-date application system architecture diagrams showing key components of the application system (e.g., active modules, database servers, application servers, access servers, etc.) and interconnectivity with other applications systems (including communication protocols and access controls). Diagrams must also show the flow of sensitive data among application components and inter-connected application systems.
- **Facilitate Incident Management & Evidence Preservation** – The ISO is expected to manage and track incident via the designated University incident system and provide access based on need to know (e.g., to the DSIRT, affected unit, system owners and administrators). The ISO should provide direction and oversight for forensically sound collection of evidence. The ISO should provide direction and oversight for storage and chain of custody tracking of evidence as needed.
- **Conduct Training and Drills** – The ISO is expected to provide ongoing realistic incident response training for data stewards, system owners and administrators, including incident prevention steps, common indicators of compromise, first-responder actions, acceptable containment, eradication and recovery steps. The ISO is also expected to conduct ongoing incident response drills to ensure that the DSIRT and other key stakeholders are well versed in how to perform their duties when the need arises. ***System owners and administrators should document high-risk incident scenarios and plan containment, eradication and recovery steps***.
- **Maintain Key Contacts List** – The ISO is expected to maintain a list of key contacts required during incident response activities. This includes contacts for DSIRT members, backup members, Cyber insurance company, support vendors, state and federal support partners, etc.

Preapproved Incident Response

The ISO, Office of General Counsel and University Communication departments should retain preapproved vendors – as part of our cybersecurity insurance policy – to provide support as needed during an incident. Contacts and procedures related to each vendor should be maintained within the central DSIRT information. These vendors include:

- External counsel
- Computer forensics experts
- Crisis communication management

Prevention

The most effective incident response strategy is to prevent incidents from occurring in the first place. To minimize the risk of incidents occurring, data stewards must ensure that effective security controls are implemented to protect systems that process, store or transmit their data. Refer to the **University of Oregon Information Asset Classification and Management Policy** for the minimum security controls required based on the classification of data processed, stored or transmitted by each system.

Phase II – Incident Handling

There are five key objectives of the Incident Handling phase of the incident response procedure – detection, analysis, investigation and containment, eradication and recovery, and post-incident activity. Activities for meeting each objective follow.

Detection

All suspected breaches or unauthorized disclosures of sensitive data must be reported by sending an email to the ISO at **infosec@uoregon.edu** or by calling our office at **(541) 346-5837**. Data security breaches or unauthorized disclosures may occur in a variety of ways. The following is a list of common ways that these incidents may occur and means by which they may be discovered:

- **Malware infection** of systems which process, store or transmit sensitive data, potentially allowing unauthorized access or retrieval of data; typically discovered by system users, automated antivirus or network monitoring tools.
- **Backdoors** installed by hackers on systems with sensitive data, giving them unauthorized remote access to the systems for harvesting the data; typically discovered by security monitoring or scanning tools or by reviewing of system logs by IT administrators.
- **Accidental disclosure** on a public or internal website, over the phone, or through physical or electronic mailing or faxing. Please report any accidental disclosure of sensitive information to the ISO (even if the disclosed item was deleted), so that any remnants can be properly cleaned up.
- **Accidental sharing** of sensitive information to unapproved individuals through email, or cloud-based applications such as Microsoft OneDrive, GoogleDrive, DropBox, Box, etc. Please report any accidental sharing of sensitive information to the ISO (even if the share was removed) so that steps can be taken to clean up any potential disclosure.
- **Payment card fraud** involving skimming devices at point of sale terminals.
- **Lost or stolen physical assets** such as sensitive paper documents or computing equipment/device (laptop, PC, smartphone, tablet, USB stick, or backup media). Note: mobile equipment should be properly encrypted and password-protected to prevent sensitive data breach if lost or stolen.
- **External Partners** including state or federal agencies, cloud vendors, industry partners and others may become aware of data breaches or disclosures that affect the UO; any such report from an external agency, vendor or partner must be promptly reported to the ISO or the UO Office of General Counsel.

Upon detection (or notification) of a potential incident, the ISO:

- Coordinates with applicable system owners and administrators to identify potentially impacted sensitive data and systems.
- Performs initial scoping and incident assessment to determine the likelihood that a security incident did occur that may have affected sensitive data, and identify potential systems affected. A memory snapshot (memory dump) is usually done at this stage, without much disruption of service, for quick analysis for malware or well-known backdoors installed by hackers.
- If the determination is made that sensitive data was not affected, the incident is treated as a normal IT support issue and is advanced to the Eradication & Recovery phase of the incident response process.

Analysis

Security incidents in which sensitive data was potentially affected must be carefully analyzed and investigated to ensure compliance with UO policies, state, federal laws and international laws, and contractual agreements.

Following are key activities conducted during this phase of the incident lifecycle by the **ISO with assistance from System Owners and Administrators**:

- **Incident timeline tracking.** The ISO must ensure that an accurate timeline of key activities is maintained throughout the lifecycle of an incident.
- **Hard drive cloning.** In addition to the memory dump collected in the Detection phase, it may be necessary to collect images of hard drives (“cloning”) of affected systems, which often causes disruption in service due to possible system reboots.
- **Evidence chain of custody tracking.** During analysis, the ISO must take steps to ensure that original evidence remains unchanged using careful chain of custody tracking and hashing algorithms.
- **Basic analysis**. The ISO performs basic forensic analysis of primary system’s memory, hard drives, network and system logs and other sources of evidence to determine the potential impact of the incident.
- **Preliminary security incident report**. A preliminary report is created following basic analysis; results documented in this report are used by the CISO to determine if the DSIRT should be activated.

Following are key activities conducted during this phase of the incident lifecycle **by the DSIRT**:

- **Assess potential breach** to ensure that all relevant stakeholders are engaged in the incident response process.
- **Cybersecurity insurance engagement** to assess if the incident warrants a cyber-insurance claim and determine whether optional insurance services, such as call center, legal services, forensics expertise, or public relations services, will be needed.
- **Coordinate and oversee communication.** The team begins the process of identifying affected parties and coordinating internal and external communication activities.

Investigation & Containment

Following are key activities conducted during this phase of the incident lifecycle by the **ISO with assistance from System Owners and Administrators**, in collaboration with external partners (e.g., law enforcement, cloud vendors, forensic firms) as needed:

- **Containment** activities should be approached in a methodical manner to avoid contamination of evidence. Caution should be exercised to avoid activation of malicious scripts that could destroy evidence, affect impacted systems or other systems in production. ***Ideally, containment actions should be based on those pre-planned by the system owners and administrators during the Planning and Preparation phase.***
- **Common containment options** depending on the situational attributes of the incident include one or more of the following:
    - Disabling of compromised accounts, or downgrading privileges.
    - Temporarily disabling affected services or disconnecting the system from the network.
    - If supported, remotely erasing or wiping system hard drives for lost or stolen equipment such as mobile phones, laptops, and tablets.
    - Quarantining affected systems from the Internet and the UO network.
    - Disabling affected system functions.
    - Note: to preserve electronic evidence, **do not shut down, reboot, disconnect from the network, access or otherwise alter the affected system before consulting with the ISO**.
- **Forensic investigation.** A primary goal of this phase is to minimize service downtime and avoid contamination of evidence by performing containment and forensic investigative activities in parallel (where possible). For example, forensic copies of evidence should be used during investigation so that work can be done to contain issues on the primary systems and return unaffected services to operational status.
- **Data Exfiltration**. The key output expected from this phase is to determine if data exfiltration occurred by reviewing systems and network logs and other sources of evidence.
- **Detailed Security Incident Report**. A detailed report must be created outlining results of the investigative analysis, status of containment activities, and recommendations for eradication and recovery; the intended audience of this report is the DSIRT.

Following are key activities conducted during this phase of the incident lifecycle by the **DSIRT:**

- **Internal communication.** Approve communication and timing for internal stakeholders.
- **Reporting and notifications.** Review the Detailed Security Incident Report, determine whether a data breach or unauthorized disclosure occurred, whether the following actions are warranted under applicable law, and approve applicable actions:

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

- **Approve notifications**. Review and approve notifications to all parties. ***The head of the unit in which the breach occurred is responsible for sending notifications to affected customers***.
- **Approve eradication and recovery**. Review and approve eradication and recovery steps recommended in the Detailed Security Incident Report.

Integration with the University Incident Management Team (IMT)

Depending on the severity of risk involved with the incident, the DSIRT may be folded into the University Incident Management Team (IMT). The decision for escalation to the IMT for cyber incidents will be made by the University CISO and the Chief Resilience Officer (CRO).

Eradication & Recovery

The objective of this phase is to rid the UO network and systems of the vulnerabilities or weaknesses that were exploited to cause the incident, and to restore all services to operations with an enhanced security posture. Note: depending on the nature of the incident, this phase could take several weeks or even months to accomplish. ***Eradication and Recovery must be performed with oversight by DSIRT*.**

Following are potential activities (depending on situational attributes of the incident) conducted during this phase of the incident lifecycle by the **system owners and administrators** with oversight by the ISO**:**

- **Eradication**. Depending on the incident, one or more of the following may be done to address near-term issues:
  - Disable compromised accounts, change passwords, and/or require two-factor authentication.
  - Quick scans to identify and remediate vulnerabilities, malware or other indications of compromised systems.
  - Correct minor configuration weaknesses and/or apply quick patches to affected systems.
- **Recovery**. Depending on the incident, one or more of the following may be done to address longer-term issues:
  - Rebuild, reimage or restore system with enhanced security controls (e.g., host-based firewall, network firewall, encryption).
  - Upgrade systems and software to secure versions.
  - Overall security assessment of the unit and/or services impacted, including ongoing extensive (privileged) vulnerability scanning and remediation.

    - Enable system and applications logging to central logging, monitoring and alerting service.

- **Root Cause Analysis**. Perform analysis to identify and address the root cause of the incident (e.g., inadequate patch management, immature configuration management, lack of training).

Post-Incident Activity

The purpose of post-incident activities is to evaluate the effectiveness of our response to the incident, to evolve the process to address current and emerging threats and identify opportunities for leveraging advances in tools and defense techniques. Lessons learned from post-incident activities should inform changes to the Planning and Preparation phase of the process.

Following are key activities conducted as part of the post-incident activity phase, **by the DSIRT**:

- **Lessons Learned**. Review the response to the incident and identify what worked and what did not. Key questions to address in this review include:
    - How well was the incident response procedure followed?
    - Are there parts of the incident response procedure that did not work and need improvement?
    - How well did each player (ISO, DSIRT, unit, sys admins, external partners, etc.) perform? Are there opportunities for improvement (e.g., training, service level modifications)?
    - How can we limit the cost of similar incidents in the future?
    - What leading indicator should we watch for in the future to improve detection?
    - Are there strategy shifts to recommend to the ISO and Information Security and Privacy Governance subcommittee (ISP GC)?
- **Evidence retention**. The ISO works with OGC to assess requirements for evidence retention and works with applicable stakeholders to meet those requirements. Note: costs for storage of evidence could be significant depending on the scope and type of incident.
- **Metrics**. The ISO documents and records key metrics of the incident and reports to the DSIRT. Key metrics include:
    - Total cost of the incident (including insurance co-pays, people-hours, settlements/fines/penalties, productivity loss, intellectual property loss, vendor services, notification/credit monitoring costs, etc.).
    - Time to detect incident; i.e., how long after the incident occurred did we find out?
    - Number of sensitive records impacted.
    - Time to notify affected customers.
    - Time to notify state and federal agencies and contractual partners.

Financial 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 to the degree that they are deemed responsible for the exposure by the DSIRT.

Reference

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

Student Records	University Registrar
Personnel Files	Chief Human Resources Officer
Sensitive Financial Records	AVP Business Affairs
Private Personal Information (PPI) - e.g., grievance information, medical information, FMLA information, military status, etc.	University Registrar, Human Resources, Library, Advancement, Others
Personally Identifiable Information (social security numbers, credit card and bank account numbers, etc.)	University Registrar, Human Resources, Library, Advancement, Others
Protected Health Information (PHI)	HIPAA Covered Entities
Identifiable Human Subject Data	Principal Investigators

The full listing of data types, descriptions, and Data Stewards are available in the University Data Security Classification Table.

Review

Last updated: May 2019.
This procedure will be reviewed at least once every two years.