Information Technology
Incident Response Plan

Revision History

Revision	Change	Date
1.0	Initial Incident Response Plan	8/28/2013
1.1	Updated to remove OUS references, position changes	9/21/2017

Official copies of the document are available at the following locations:

- Department of Information Technology Office
- Office and home of the Chief Information Officer

Contents

Section 1: Introduction

Faculty, staff, and students of Southern Oregon University all rely heavily on the Information Technology (IT) infrastructure and services to accomplish their work and as an integral part of

the learning environment.

As a result of this reliance, IT services and data maintained on IT systems are considered a critical component in the daily operations of Southern Oregon University, requiring a comprehensive Incident Response Plan to assure that these services and data remain as secure as possible.

This plan outlines the steps to follow in the event secure data is compromised and identifies and describes the roles and responsibilities of the Incident Response Team. The Incident Response Team is responsible for putting the plan into action.

This plan is reviewed and updated annually by IT staff and approved by the Chief Information Officer

A copy of this plan is stored in the following areas:

- Department of Information Technology Office
- Office and home of the Chief Information Officer

Section 2: Scope

This plan covers all phases of response to a data security breach occurring at Southern Oregon University. These phases include:

- Incident Reporting
- Incident Response
- Notification
- Post incident Review

Section 3: Assumptions

This incident response plan is based on the following assumptions:

Once an incident covered by this plan has occurred, the appropriate priority will be given to the response effort and the resources and support required as outlined in the IT Incidence Response Plan will be available.

Depending on the severity and type of security breach, other departments/divisions on campus may be required to modify their operations to accommodate any changes in system availability and data access until a full recovery has been completed. Information Technology will encourage all other departments to have contingency plans and Business Continuity Plans for their operations, which include operating without IT systems for an extended period of time. In addition, permanent changes in department/division or university operations may be required to mitigate breach recurrence or to mitigate ongoing security risks.

The content of this plan may be modified and substantial deviation may be required in the event

of unusual or unforeseen circumstances. These circumstances are to be determined by the Incident Response Team under the guidance and approval of the Chief Information Security Officer.

Section 4: Need for Incident Response

Incident response has become necessary because attacks frequently cause the compromise of personal and university data. Incidents involving viruses, worms, Trojan horses, spyware, and other forms of malicious code have disrupted or damaged millions of systems and networks around the world. Breaches and exposure of personally identifiable information (PII) at other universities have resulted in significant legal settlements and have raised awareness of the possible effects of computer-based attacks. These events—and many more—make the case daily for responding quickly and efficiently when computer security defenses are breached. To address these threats, the concept of computer security incident response has become widely accepted and implemented in the Federal government, private sector, and academia.

The following are benefits of having an incident response capability:

- Responding to incidents systematically so that the appropriate steps are taken
- Helping university employees to recover quickly and efficiently from security breaches, minimizing loss or theft of information and disruption of services
- Using information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data
- Dealing properly with legal issues that may arise during incidents.

Section 5: Definition of a Security Breach

A security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personally identifiable information (PII) maintained by Southern Oregon University. Good faith acquisition of personally identifiable information by an employee or other authorized user for university purposes is not a breach, provided that the information is not used or subject to further unauthorized disclosure.

Personally identifiable information includes any data that can be linked to an individual or used to directly or indirectly identify an individual. Most information that the university collects about an individual is likely to be considered personally identifiable information.

For our purposes, personally identifiable information is defined as an individual’s first name or first initial and last name, in combination with any of the following data:

- Driver’s license number or state-issued identification card number
- Family Educational Rights and Privacy Act (FERPA) protected information
- Financial account number, credit, or debit card number
- Home address or e-mail address

- Medical or health information
- Passwords
- Social Security Number

Section 6: Reporting an Incident

For Southern Oregon University, the most challenging part of the incident response process is accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem. What makes this challenging is a combination of three factors:

- Incidents may be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based intrusion detection systems, antivirus software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect without automation.
- The volume of potential signs of incidents is typically high; for example, it is not uncommon for SOU to receive thousands of penetration and port scanning attempts per day.
- Deep, specialized technical knowledge and extensive experience are necessary for proper and efficient analysis of incident-related data.

A security breach might result from any or all of the following events:

- Denial of Service (DoS)—an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources
- Malicious Code—a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host
- Unauthorized Access—a person gains logical or physical access without permission to a network, system, application, data, or other IT resource
- Inappropriate Usage—a person violates the SOU Acceptable Use Policy
- Multiple Component—a single incident that encompasses two or more incidents; for example, a malicious code infection leads to unauthorized access to a host, which is then used to gain unauthorized access to additional hosts.

If you suspect a security breach or unauthorized release of personally identifiable information has occurred, you must report it as soon as possible to the Information Technology department or directly to the Chief Information Security Officer/Chief Information Officer.

Section 7: Teams

7.0.1 Chief Information Security Officer

Chief Information Security Officer	
Home Phone:	
Cell Phone:	

7.0.2 Incident Response Command Team

Chief Information Officer	
Manager, Infrastructure Services	
Manager, Information Systems	

7.1 Incident Response Team

All Contact Information is located in Appendix A

The role of the Incident Response Team is to provide a quick, effective and orderly response to computer related incidents such as virus infections, unauthorized network and server access,

improper disclosure of confidential information to others, security related service interruptions, breach of personal information, and other events with serious information security implications.

The Incident Response Team will take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to the university leadership and the appropriate authorities as necessary. The Chief Information Security Officer will coordinate these investigations.

Team Lead:	Chief Information Security Officer
Team Members:	Manager, Information Systems
	Manager, Infrastructure Services
	Desktop Systems Administrator
	System Administrators (2)
	Web Programmer/Analyst
	Programmer/Analyst

7.2 Critical Southern Oregon University and Oregon University System Contacts

A copy of the Southern Oregon University Emergency Response Contacts List is located in Appendix B

Vice President for Finance and Administration	
SOU General Counsel	
SOU Internal Auditor	

Section 8: Incident Response Procedures

8.1 Notice of Potential Breach:

This Incident Response Plan outlines steps that SOU will take upon notice or discovery of potential unauthorized access to personally identifiable information (PII).

The CISO will serve as a central point of contact for reporting any suspected or confirmed breach of PII.

After receiving notification of potential unauthorized access or disclosure of PII, the CISO will perform a preliminary analysis of the facts and assess the situation to determine the nature and

scope of the incident. Additionally, the CISO will:

a. Inform the Vice President for Finance and Administration that a possible privacy breach has been reported and provides them an overview of the situation.
b. Contact the person(s) who reported the problem.
c. Identify the systems and type(s) of information affected and determine whether the incident could be a breach or suspected breach of personal information about an individual. Every breach may not require participation of all Incident Response Team members (e.g., if the breach was a result of hard copy disposal or theft, the investigation may not require the involvement of system administrators and other technical support staff).
d. If applicable, review the preliminary details with the IT manager of the implicated system(s).
e. Activate the Incident Response Team if a privacy breach affecting personal information is confirmed.
f. Begin an Incident Report (Appendix C)
g. Update the Vice President for Finance and Administration on the status of the incident.
h. Notify the Internal Auditor of the security breach, if they have not already been notified by the Vice President for Finance and Administration.
i. Complete the Incident Report and close the incident if no breach of PII occurred.

8.2 Incident Response Team Actions:

Once it has been determined that a breach or unauthorized access of PII has occurred, the Incident Response Team will begin assessing the breach, its severity, remedial steps necessary to prevent ongoing unauthorized access, and consult with other university personnel regarding notification requirements and actions.

The Incident Response Team is responsible for documenting all details of an incident and facilitating communication to other university staff as needed. Team members must keep accurate notes of all actions taken, by whom, and the exact time and date. Each person involved in the response must record his or her own actions. The Team will:

a. Work with the appropriate parties to determine the extent of the potential breach. Identify data stored and compromised on all test, development and production systems and the number of individuals at risk.
b. Identify and contact the appropriate Data Owner (Records Custodian) affected by the breach.
c. Contact all appropriate database and system administrators to assist in the investigation effort (i.e. USSE Site staff)
d. Determine the type of personal information that is at risk, including but not limited to:
    - Driver’s license number or state-issued identification card number

- Family Educational Rights and Privacy Act (FERPA) protected information
- Financial account number, credit, or debit card number
- Home address or e-mail address
- Medical or health information
- Passwords
- Social Security Number

e. Have the Data Owner (Records Custodian) determine what records might be affected. Engage other IT staff as necessary to help make these determinations. Identify individuals whose information may have been compromised. An assumption could be "all" if an entire table or file was compromised.
f. Determine if an intruder has exported or deleted any personal information data.
g. Determine where and how the breach occurred. Identify the source of compromise, and the timeframe involved. Review the network to identify all compromised or affected systems. Consider e-commerce third party connections, the internal corporate network, test and production environments, virtual private networks, and modem connections. Look at appropriate system and audit logs for each type of system affected. Look at directory and file permissions. Document all internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.
h. Take measures to contain and control the incident to prevent further unauthorized access to or use of personal information on individuals, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls. Change all applicable passwords for IDs that have access to personal information, including system processes and authorized users. If it is determined that an authorized user's account was compromised and used by the intruder, disable the account. Do not access or alter the compromised system. Do not turn off the compromised machine. Isolate the system from the network (i.e., unplug cable).
i. Monitor systems and the network for signs of continued intruder access.
j. Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the format and platform used is suitable for review and analysis by a court of law if needed. Document all actions taken, by whom, and the exact time and date. Each employee involved in the investigation must record his or her own actions. Record all forensic tools used in the investigation.
k. Update the Incident Report. Provide a summary of confirmed findings and of the steps taken to mitigate the situation to involved parties.

Additional steps to be taken by the CISO include:

a. If the breach occurred from a third party, determine if a legal contract exists. Work with Business Services, general counsel, and, if necessary, the Data Owner (Records Custodian) to review contract terms and determine next course of action.
b. If credit cardholder data is involved, determine third-party reporting requirements with Business Services (Bursar).
c. Determine notification requirements (see Section 8)
d. If an internal user (authorized or unauthorized employee, contractor, consultant, student employee, etc.) was responsible for the breach, contact the Vice President of Finance and Administration, the appropriate department director, Student Conduct Coordinator, and/or Human Resources.
e. Coordinate next steps with the Vice President of Finance and Administration, the internal auditor, and the general counsel.

8.3 Responsibilities of Data Owners (Records Custodians):

a. If notified of a potential breach affecting personally identifiable information (PII), contact the Chief Information Security Officer (CISO) immediately.
b. When notified by the CISO that the Incident Response Plan has been activated, perform a preliminary analysis of the facts and assess the situation to determine the nature of the incident.
c. Work with the CISO and the Incidence Response Team to identify the extent of the breach.
d. If appropriate, notify your staff that a breach has been reported and is under investigation.
e. Work with your staff to ensure there is no further exposure to unauthorized access or disclosure of personally identifiable information (PII).

Section 9: Notification Process

Federal and state law and university policy requires notification to individuals affected by unauthorized access or release of personally identifiable information.

The Chief Information Security Officer will coordinate with the Vice President of Finance and Administration, the Data Owner (Records Custodian), the Internal Auditor, general counsel, and, if necessary, Marketing and Communications to determine notification requirements.

The Data Owner (Records Custodian) will be responsible for notifying affected individuals. A sample notification letter is included in Appendix D.

The following list includes selected state laws and university regulations governing notification requirements. This should not, however, be considered a complete list.

Oregon Consumer Identity Theft Protection Act

http://www.oregon.gov/DAS/OSCIO/Pages/Security.aspx

http://www.oregon.gov/das/OSCIO/Documents/notification_bestpractices.pdf

SOU Information Security Policy

http://www.sou.edu/policies/Information-Security.pdf

SOU Information Security Procedure

https://inside.sou.edu/assets/it/docs/information-security-procedure.pdf

Appendix A. IT Contact List

This page considered confidential. A paper copy of the IT Contact List is attached to this document in its official locations. The electronic version of this list is available in Google Drive (access is restricted).

Appendix B. Southern Oregon University Crisis Management Team Contact List

This page considered confidential. A paper copy of the Southern Oregon University Crisis Management Team Contact List is attached to this document in its official locations. The electronic version of this list is available in Google Drive (access is restricted).

Appendix C. Incident Report Form

The electronic version of this form is available in Google Drive (access is restricted to SOU personnel only).

Appendix D. Sample Notification Letter

The electronic version of the sample notification letter is available in Google Drive (access is restricted).