

Information Security Incident Response Plan



Agency: Oregon Military Department

Date: 12 April 2010

Contact: Director of Financial Administration (OMD Chief Information Officer)

TABLE OF CONTENTS

Introduction	2
Authority	3
Terms and Definitions	3
Roles and Responsibilities	4
Program	4
Education and Awareness	7
Communications	7
Compliance	8
Implementation	9
Approval	9

Introduction

ORS 182.122 requires agencies to develop the capacity to respond to incidents that involve the security of information. Agencies must implement forensic techniques, remedies and consider lessons learned. The statute also requires reporting incidents and plans to the Enterprise Security Office. The Oregon Consumer Identity Theft Protection Act (ORS 646A.600) requires agencies to take specific actions in cases where compromise of personally identifiable information has occurred. This plan addresses these requirements.

The Oregon Military Department (OMD) has developed this Information Security Incident Response Plan to implement its incident response processes and procedures effectively and to ensure that OMD employees understand them. The intent of this document is to:

- describe the process of responding to an incident,
- educate employees, and
- build awareness of security requirements.

An incident response plan incorporates and organizes the resources for dealing with any event that harms or threatens the security of information assets. Such an event may be a malicious code attack, an unauthorized access to information or systems, the unauthorized use of services, a denial of service attack, or a hoax. The goal is to facilitate quick and efficient response to incidents and to limit their impact while protecting the state's information assets. The plan defines roles and responsibilities, documents the steps necessary for effectively and efficiently managing an information security incident, and defines channels of communication. The plan also prescribes the education needed to achieve these objectives.

Authority

Statewide information security policies:

Policy Number	Policy Title	Effective Date
107-004-050	Information Asset Classification	1/31/2008
107-004-051	Controlling Portable and Removable Storage Devices	7/30/2007
107-004-052	Information Security	7/30/2007
107-004-053	Employee Security	7/30/2007
107-004-100	Transporting Information Assets	1/31/2008
107-004-110	Acceptable Use of State Information Assets	10/16/2007
107-004-120	Information Security Incident Response	11/10/08

OMD information security policies:

Policy Number	Policy Title	Effective Date
AGC-248.006	Acceptable Use of State Information Assets	8 April 2010
AGC-248.010	Information, Network and User Security	8 April 2010
AGC-248.017	Information Security Incident Response	12 April 2010

Terms and Definitions

Asset: Anything that has value to the agency

Control: Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or of legal nature

Incident: A single or a series of unwanted or unexpected information security events (see definition of "information security event") that results in harm, or poses a significant threat of harm to information assets and requires non-routine preventative or corrective action.

Incident Response Plan: Written document that states the approach to addressing and managing incidents.

Incident Response Policy: Written document that defines organizational structure for incident response, defines roles and responsibilities, and lists the requirements for responding to and reporting incidents.

Incident Response Procedures: Written document(s) of the series of steps taken when responding to incidents.

Incident Response Program: Combination of incident response policy, plan, and procedures.

Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, including electronic, paper and verbal communication.

Information Security: Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Information Security Event: An observable, measurable occurrence in respect to an information asset that is a deviation from normal operations.

Threat: A potential cause of an unwanted incident, which may result in harm to a system or the agency

Roles and Responsibilities

OMD Deputy Director Responsible for information security in the agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the enterprise. The director also is responsible for ensuring compliance with state enterprise security policies, standards, and security initiatives, and with state and federal regulations.

OMD Chief Information Officer (CIO) The CIO is also responsible for administering and managing the Incident Response when an incident occurs. The OMD CIO also serves as the Director of Financial Administration.

OMD Information Security Officer (ISO) **Is the agency's Incident Response Point of Contact** Responsible for communicating with State Incident Response Team (SIRT) and coordinating agency actions with SIRT in response to an information security incident.

Information Owner Responsible for creating initial information classification, approving decisions regarding controls and access privileges, performing periodic reclassification, and ensuring regular reviews for value and updates to manage changes to risk.

User Responsible for complying with the provisions of policies, procedures and practices.

Program

The Incident Response Program is composed of this plan in conjunction with policy and procedures. The following documents should be reviewed for a complete understanding of the program:

1. OMD Information Security Incident Response, Policy Number AGC-248.017
2. OMD Acceptable Use of State Information Assets, Policy Number AGC-248.006
3. OMD Information, Network and User Security, Policy Number AGC-248.010

Information security incidents will be communicated in a manner allowing timely corrective action to be taken. This plan shows how the OMD will handle response to an incident, incident communication, incident response plan testing, training for response resources and awareness training

The OMD CIO will conduct an annual review of the Information Security Incident Response policy, plan and procedures. A review will take place if significant changes occur to ensure their

continuing adequacy and effectiveness. Reviews will include assessing opportunities for improvement and approach to managing information security incident response in regards to integrating lessons learned, to changes to OMD's environment, new threats and risks, business circumstances, legal and policy implications, and technical environment.

Identification

Identification of an incident is the process of analyzing an event and determining if that event is normal or if it is an incident. An incident is an adverse event and it usually implies either harm, or the attempt to harm OMD. The OMD ISO routinely examines events to determine their impact and their potential for harm. The OMD ISO is responsible for identification of an incident.

The term "incident" refers to an adverse event impacting one or more OMD's information assets or to the threat of such an event. Examples include but are not limited to the following:

- Unauthorized use
- Denial of Service
- Malicious code
- Network system failures (widespread)
- Application system failures (widespread)
- Unauthorized disclosure or loss of information
- Information Security Breach
- Other

Incidents can result from any of the following:

- Intentional and unintentional acts
- Actions of state employees
- Actions of vendors or constituents
- Actions of third parties
- External or internal acts
- Credit card fraud
- Potential violations of Statewide or OMD's Policies
- Natural disasters and power failures
- Acts related to violence, warfare or terrorism
- Serious wrongdoing
- Other

Incident Classification

Once the OMD ISO determines an event to be an incident, several methods exist for classifying the incident. The OMD ISO considers the following factors when evaluating incidents:

- Criticality of systems that are (or could be) made unavailable
- Value of the information compromised (if any)
- Number of people or functions impacted
- Business considerations

- Public relations
- Enterprise impact
- Multi-agency scope

Triage

The objective of the triage process is to gather information, assess the nature of an incident and begin making decisions about how to respond to it. Preventing the situation from becoming more severe is critical. The following factors receive consideration during triage:

- What type of incident has occurred
- Who is involved
- What is the scope
- What is the urgency
- What is the impact thus far
- What is the projected impact
- What can be done to contain the incident
- Are there other vulnerable or affected systems
- What are the effects of the incident
- What actions have been taken
- Recommendations for proceeding
- May perform analysis to identify the root cause of the incident

Evidence Preservation

Carefully balancing the need to restore operations against the need to preserve evidence is a critical part of incident response. Gathering evidence and preserving it are essential for proper identification of an incident, and for business recovery. Follow-up activities, such as personnel actions or criminal prosecution, also rely on gathering and preserving evidence.

The OMD ISO is responsible for leading efforts to preserve evidence. Should additional expertise prove necessary, the OMD ISO will contact the State of Oregon's Electronic Security Office (ESO).

Forensics

If an incident involves computers, the OMD ISO will technically analyze computing devices to identify the cause of an incident or to analyze and preserve evidence.

OMD will practice the following general forensic guidelines:

- Keep good records of observations and actions taken.
- Make forensically-sound images of systems and retain them in a secure place.
- Establish chain of custody for evidence.
- Provide basic forensic training to incident response staff, especially in preservation of evidence

Threat/Vulnerability Eradication

After an incident, efforts will focus on identifying, removing and repairing the vulnerability that led to the incident and thoroughly clean the system. To do this, the vulnerability(s) needs to be clearly

identified so the incident isn't repeated. The goal is to prepare for the resumption of normal operations with confidence that the initial problem has been fixed. Data owners are responsible for working with the OMD ISO to develop and implement a remediation plan for every incident.

Confirm that Threat/Vulnerability has been Eliminated

After the cause of an incident has been removed or eradicated and data or related information is restored, it is critical to confirm all threats and vulnerabilities have been successfully mitigated and that new threats or vulnerabilities have not been introduced. The OMD ISO and data owner will be jointly responsible for confirming elimination of all threats and vulnerability.

Resumption of Operations

Resuming operations is a business decision, but the preceding steps are critical to ensure that resuming operations are safe. Division Directors and/or Program Managers must consult with data owners to decide when resumption will occur. Division Directors or Program Managers have responsibility for notifying the OMD ISO that the incident is closed.

Post-incident Activities

Following every incident, the OMD ISO will lead an after-action analysis. The analysis may consist of one or more meetings and/or reports. The purpose of the analysis is to give participants an opportunity to share and document details about the incident and to facilitate lessons learned. The meetings should be held within one week of closing the incident.

Education and Awareness

User awareness of OMD's policies, procedures and plans surrounding Information Assets, Security and Incident Responses is established by links on the agency's home page. All OMD users will review these policies upon hire and at least annually thereafter. OMD will be establishing training opportunities using ILearn.

Communications

Because of the sensitive and confidential nature of information and communication surrounding an incident, all communication must be through secure channels. The OMD CIO and ISO will provide incident briefings to the OMD Deputy Director, who will determine the levels and involvement of communications surrounding an incident.

Details of an incident should only be communicated face-to-face or by phone. Do not communicate details of an incident by e-mail, voice message, or interagency shuttle mail. If you must exchange reports and data electronically, use encryption. Label all relevant material ***"Confidential: Exempt from Public Records Law."***

Among the factors to be considered when developing a communications plan are the following:

- Requirements of the Oregon Consumer Identity Theft Protection Act (note: actions taken in response to violations or potential violations of this Act must be coordinated in advance with the (DAS) Enterprise Security Office).
- Requirements of regulations such as Payment Card Industry – Data Security Standards (PCI-DSS), Health Insurance Portability and Accountability Act (HIPPA), Internal Revenue Service regulations, etc.
- Additional risks occurred by releasing specific incident information
- Asset classification level of the information involved in the incident
- Agency credibility

- Determining who needs to know various levels of detail
- Managing the message in a positive manner

If required, the Oregon National Guard Public Affairs Office (PAO) will be responsible for media relations during incidents. No employee, user or authorized representative of the Oregon Military Department may discuss an incident with anyone until receiving specific approval from the PAO, OMD CIO, Deputy Director, or The Adjutant General.

Only the following people should receive reports of the details of any incident:

- Those who need the information to conduct the investigation
- Those who need the information to take corrective action
- Those who need the information to prepare a communications plan

The purpose of limiting the flow of information is to contain risks to compromised systems, the agency, or customers and vendors.

Depending on the circumstances of an incident, the following contacts may be relevant:

Contact	Phone Number
OMD ISO	503.584.3911
OMD CIO	503.584.3875
Deputy Director	503.584.3884
State Chief Information Security Officer	503.378.4896
Oregon State Police Criminal Lieutenant	503.378.3720
Department of Justice	503.947.4540
DAS Risk Management	503.373.7475
If security breach affects more than 1,000 consumers, contact all major consumer-reporting agencies that compile and maintain reports on consumers on a nationwide basis; inform them of the timing, distribution and content of the notification given to the consumers.	
Contact the credit monitoring bureaus in advance if directing potential victims to call them:	
• Equifax	1.800.525.6285
• Experian	1.888.397.3742
• TransUnion	1.800.680.7289

Compliance

OMD is responsible for implementing and ensuring compliance with all applicable laws, rules, policies, and regulations.

- ORS 182.122 – Information Systems Security in Executive Department
- ORS 646A.600 – Oregon Consumer Identity Act. OMD maintains personal information of consumers, employees, volunteers, Oregon National Guard soldiers and airmen, and their families, and individuals and their families and mentors associated with the Oregon Youth Challenge Program. OMD will notify affected persons if personal information has been subjected to a security breach in accordance with the Act. The notification will occur soon as possible, in one of the following manners:
 - Written notification
 - Electronic, if this is the customary means of communication with the affected person
 - Telephone notice provided that can directly contact the affected person.

Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation.

If an investigation into the breach or consultation with a federal, state or local law enforcement agency determines there is no reasonable likelihood of harm to consumers, or if the personal information was encrypted or made unreadable, notification is not required.

Substitute notice

If the cost of notifying customers would exceed \$250,000, that the number of those who need to be contacted is more than 350,000, or if there isn't means to sufficiently contact consumers, substitute notice will be given. Substitute notice consists of:

- Conspicuous posting of the notice or a link to the notice on your Web site if one is maintained, and
- Notification to major statewide Oregon television and newspaper media.

Notifying credit-reporting agencies

If the security breach affects more than 1,000 consumers OMD will report to all nationwide credit-reporting agencies, without reasonable delay, the timing, distribution, and the content of the notice given to the affected consumers.

Implementation

The OMD CIO and ISO will be responsible for reviewing, testing and implementing this plan. Review of this plan will occur annually, and testing of the plan will take place at least once every two years.

Approval

By: _____
J. Michael Caldwell, Brigadier General, Deputy Director

By: _____
Karl D. Jorgenson, Director of Financial Administration (CIO)