

**Oregon Department of Justice
Security Incident Response Plan
(Revised xx/xx/xxxx)**

Purpose

The purpose of this plan is to protect the confidentiality, integrity and availability of Department data. The proper handling of information security incidents, both electronic and physical, is critical in protecting the Oregon Department of Justice (“Department”).

The security incident response plan is organized into four stages.

Incident Identification, Containment, and Classification (*stage one*)

A security incident is a real or perceived threat which exploits or attempts to exploit a vulnerability.

All Department employees are responsible for identifying and reporting possible security incidents. While some security incidents appear to be easily identified and understood, others require review and analysis to make a determination about the nature and scope of the problem. Many Department employees will not be able to confirm a security incident, thus any abnormal events should be reported promptly. Examples of events which should be reported are:

- Password alterations not initiated by the user;
- Internet browser pop-ups that cannot be closed;
- Workstation infection from a virus, worm, spyware or other malicious software;
- Missing physical files that contain data classification Level 2, Level 3, or Level 4 information;
- Loss or theft of Department identification key cards and badges;
- Loss or theft of Department keys which allow facilities access;
- Loss or theft of Department computer hardware; and
- Loss or theft of any mobile computing device.

All Department employees must report these and other suspicious events immediately to the Customer Service Center (503) 373-7971 and to their manager during normal business hours. All after-hours security incidents must be reported as soon as possible to the employee’s supervisor. Loss or theft of Department real or personal property must be reported to the Operations Manager. The Operations Manager is responsible for implementing the Department Property Loss Policy. Security incidents will be documented on the Department’s Security Incident Response Form (Attachment G).

Here are some general guidelines that should be followed during a possible security incident:

- If your password has been compromised, change it immediately and report the security incident;
- If you have reported a security incident, do not continue working on the computer, or in the case of a physical security incident do not continue working in that area;
- Do not close computer applications, or alter the work area (close or move physical documents, etc.) as this may destroy useful information;
- Do not resume using a workstation or a work area until it is declared ‘safe’ by the Security Incident Response Team (SIRT); and
- Only discuss the security incident with the SIRT. Only the SIRT and Department management are allowed to communicate information about a security incident.

When reporting a potential security incident attention to detail is very important. Keep track of the time and what activities were being performed (in detail) when the potential security incident is discovered. By recording these facts, the SIRT will have better information by which to respond to the security incident. The important details to include in reporting a security incident are:

- Name, location, telephone number and workstation name if applicable;
- A detailed description of the potential security incident or abnormal event(s);
- The date(s) and time(s) of when the potential security incident or abnormal event occurred; and
- Any other additional information which can be obtained without affecting or making worse the security incident or which could alert a potential or confirmed perpetrator that someone is aware of their actions or presence.

The Customer Service Center will begin the documentation process and notify a SIRT member. Attachment A details the process flow in selecting a SIRT member to respond to a reported or discovered security incident.

Security incidents fall within one of three risk categories. In addition, each of these categories will be associated with a security incident classification level (Attachment C).

Risk	Description
Low	A security incident localized to no more than two individuals and which includes data classification Level 2 information. Security incidents at this level include loss of physical or electronic data which is of limited risk to the Department.
Medium	A security incident which disrupts normal work (workstation, local area network, work area). Security incidents at this level may include loss, theft, or unauthorized disclosure of data classification Level 2 or Level 3 information (but which does not include personally identifiable information). Security incidents at this level are of moderate risk to the Department.
High	A security incident which affects a large number of users or which effects data classification Level 3 or Level 4 information (including any personally identifiable information). Security incidents at this level are of extreme risk to the Department.

Investigation *(stage two)*

In the investigation stage, the SIRT will gather all known information regarding the security incident and will correlate any information regarding the current incident to any other incidents and abnormal events to determine the urgency and the scope of the issue. Criteria that determine the severity and urgency are:

- Business Criticality
- System Availability
- Data Availability
- Level of current functionality
- Effect on employee productivity
- Lack of alternative workarounds
- Data classification level of information
- Loss, theft, unauthorized disclosure of personally identifiable information

If it is determined that no security incident has occurred, the suspected incident will be labeled as an event and closed by the SIRT.

Notification/Alerting and Responding *(stage three)*

In the notification and response stage the SIRT will determine the scope of the security incident, the immediate impact, and initiate the required response. Escalation and communication alerts are the responsibility of the SIRT team. Should the security incident meet any of the following criteria, the escalation process should be immediately followed:

- Security incident has an immediate enterprise wide impact;

- Security incident meets legal requirements that require disclosure; or
- Security incident has caused a business critical service interruption.

Attachment D details the Security Incident Response Communications Plan and priorities that the SIRT will follow.

Escalation

In the event that the security incident has immediate impact on the enterprise the SIRT member investigating the security incident will promptly notify the Chief Information Officer (CIO). Certain security incidents may require reporting or alerting of outside third parties or vendors. Examples include law enforcement, the State Data Center and the Department of Administrative Services Enterprise Security Office (DAS ESO). *Any loss, theft or unauthorized disclosure of personally identifiable information must follow the notification requirements as required in the Oregon Consumer Identity Theft Protection Act. See also DOJ Policy 2-125-xxxx "Reporting Unauthorized Acquisition or Disclosure of Personal Information" and Policy x-xxx-xxxx "Reporting Property Losses."*

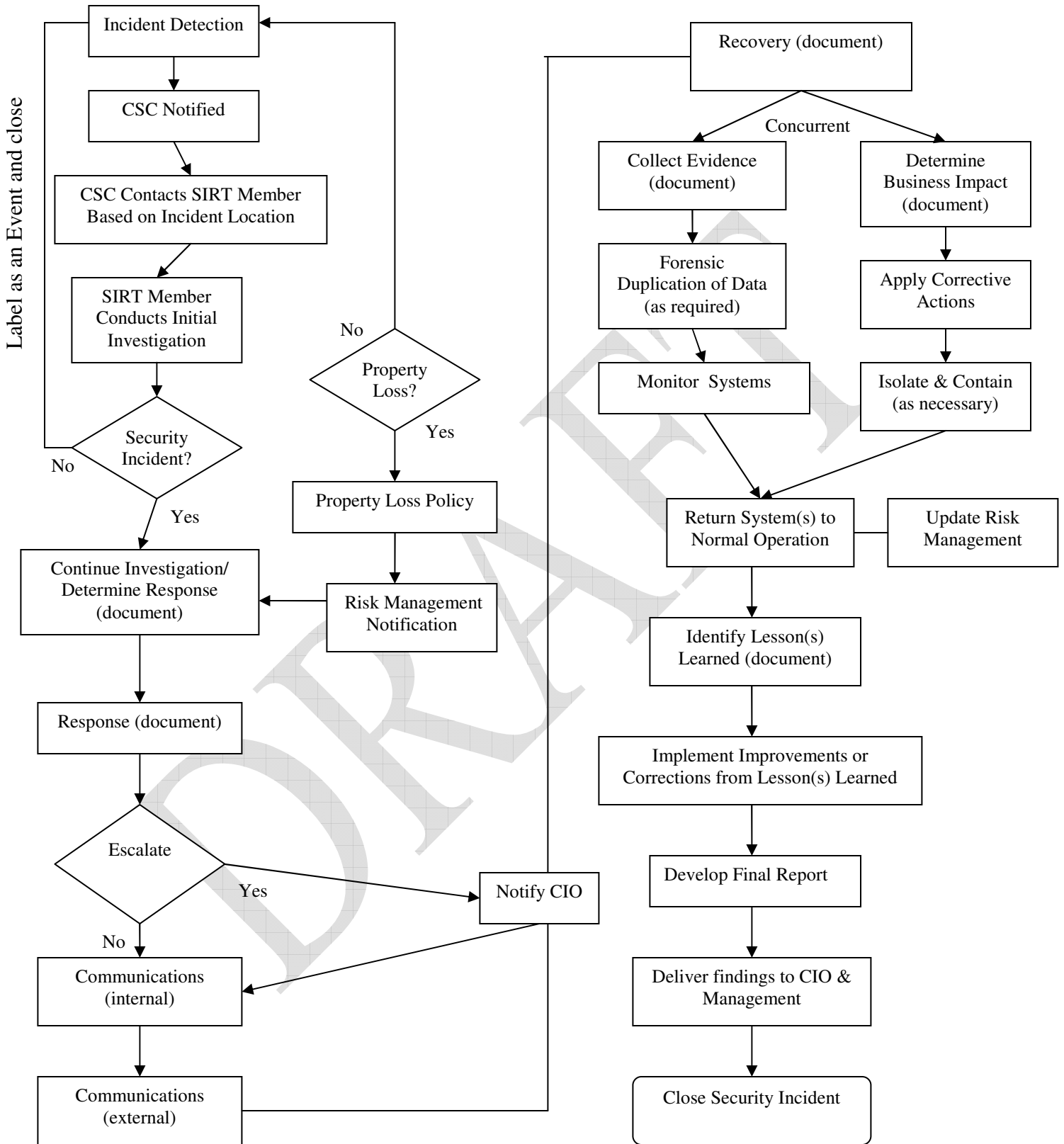
Reporting and Documentation (stage four)

All security incidents will be documented through the use of the Security Incident Response Form. All employees involved in a security incident are required to provide feedback and documentation on their involvement in the process. At a minimum, the report will contain the following information collected during each stage of a security incident investigation:

- Name, location, telephone number and workstation name if applicable;
- A detailed description of the potential security incident or abnormal event(s);
- The date(s) and time(s) of when the potential security incident or abnormal event occurred; and
- Any other additional information which can be obtained without affecting or making worse the security incident or which could alert a potential or confirmed perpetrator that someone is aware of their actions or presence;
- SIRT member who investigated the security incident;
- Cause of the security incident (if apparent);
- Employee(s) involved;
- Action(s) taken;
- Resolution;
- Date completed;
- Business impact;
- Damage caused;
- Lessons learned;
- Planned future mitigation (if possible).

Attachment E provides guidance in developing a detailed security incident response report.

Security Incident Report Process Flow¹



¹ Retention and destruction of Security Incident Response Forms are subject to OAR 166, division 300, ORS 192.001 to 192.190, and Oregon Department of Justice Special Retention Schedule 2001-0013.

Responsibility Chart

	Report	Detect/Monitor	Evaluate	Containment	Communicate	Respond/Correct	Recover	Document
Chief Information Officer	R	I	I/C/R	I/C	I/C/R	I/C	I	I/C/R
IS Management	R	I	I/C/R	I/C	I/C/R	I/C	I	I/C/R
Security Coordinator	R	C/R	I/C/R	I/C	I/C	I/C	I	I/C/R
Network Security Team Lead	R	C/R	I/C/R	C/R	I/C/R	I/C/R	I/CR	I/C/R
Network Security Administrator	R	C/R	I/C/R	C/R	I/C/R	I/C/R	I/C/R	I/C/R
Network Services Team	R	C/R	I/C/R	C/R	I/C	I/C/R	I/C/R	I/C/R
Mainframe Team	R	C/R	I/C/R	C/R	I/C/R	I/C/R	I/C/R	I/C/R
Desktop Services Team	R	C/R	I/C	I/C	I/C	I/C/R	I/C/R	I/C/R
Customer Services Team	R	C/R	I/C	I/C	I/C	I/C	I/C	I/C/R
Application Development Team	R	C/R	I/C/R	I/C/R	I/C/R	I/C/R	I/C/R	I/C/R
Division Management	R	C/R	I/C/R	I/C/R	I/C/R	I/C/R	I/C/R	I/C/R
All DOJ Employees	R	C/R	n/a	I/C	I/C	I	I	I/C
Risk Management	I	I	I/C/R	I/C/R	I/C/R	I/C	I/C	I/C/R
State Data Center (SDC related)	R	I/C/R	I/C/R	I/C/R	I/C/R	I/C/R	I/C/R	I/C/R

R = Responsible	C = Contributes	I = Informed
-----------------	-----------------	--------------

Main Responsibilities

Chief Information Officer (CIO) enforces the *Incident Response Policy* and monitors the SIRT's ability to take corrective action on security incident events. All security incidents responded to by the SIRT will be reported to the CIO.

IS Management Team supports the CIO in enforcing the *Incident Response Policy* and in monitoring the SIRT's ability to take corrective action on security incident events. Each manager has the responsibility to monitor, evaluate and provide feedback on the security incident response process. In the event that the CIO is unavailable the most senior manager available will be the CIO's backup.

Security Coordinator is assigned to evaluate and respond to security incidents. The primary responsibility of the Security Coordinator is to document the cause, detection, containment, corrective action, and recovery of security incidents responded to by the SIRT. In addition, the Security Coordinator must monitor the response process.

Network Security Team Lead is assigned to evaluate, respond, contain, correct, and recovery Department information services, data and resources from security incidents. The primary responsibility of the Network and Security Team Lead is to identify and mitigate security incidents to minimize the impact on the Department. The Network and Security Team Lead is responsible for coordinating with Desktop Support and Network Services technicians to contain, correct and recover Department information systems and data affected by the security incident.

Network Security Administrator is assigned to monitor, evaluate, respond, and contain security incidents that affect the Department. The primary responsibility of the Network Security Administrator is to assist the Network and Security Team Lead in identifying and mitigating security incidents promptly to protect the Department. The Network Security Administrator is the back-up for the Network and Security Team Lead, and is also responsible for monitoring the Department's information systems to preemptively detect security incidents.

Network Services Team will monitor, evaluate, contain, correct and recover Department information services, data and resources from security incidents that are within their area of responsibility. The Network Services Team will coordinate with the Network Security Team Lead or the Network Security Administrator as required when dealing with security incidents.

Mainframe Team is responsible for monitoring, evaluating, containing, correcting and recovering from security incidents that affect the mainframe.

Desktop Services Team will monitor and evaluate security incidents on workstations and other Department owned devices under this group's control. The Desktop Services Team will coordinate with other members of the SIRT to monitor, respond, contain, correct and recovery from security incidents that affect workstations and other Department owned devices.

Customer Service Center will typically be the first response to business reported security incidents. The Customer Service Center will document security incidents reported by the business and then determine the correct SIRT member to forward the information on to.

Application Development Team is assigned to monitor, evaluate, respond, and contain security incidents that affect the Department's applications and web services. The primary responsibility of the Development Team Lead is to respond to security incident reports on the Department's applications and web services.

Division Management will be communicated to about the nature of the security incidents, the response, containment, correction and recovery of the security incidents as it applies to their areas. Division managers will require employees to monitor, evaluate, and report security incidents that affect the Department. The Network Security Administrator is the back-up for the Network and Security Team Lead, and is also responsible for monitoring the Department's information systems to preemptively detect security incidents.

All DOJ Employees are responsible to report security incidents or suspected security incidents.

State Data Center (DAS) will be a partner in monitoring, evaluating and responding to security incidents as needed based upon Department requirements.

Oregon Department of Justice Security Incident Classification Levels

Level 1 – Low

Low level security incidents have minimal impact to information systems or data. The following are some examples of low security incidents:

- Loss, theft, or unauthorized disclosure of data that has minimal impact or risk to the Department or one of its clients;
- Vulnerabilities that can be completely mitigated by changes in configurations, policy, procedure, or through technology; and
- Loss, theft, or unauthorized disclosure of a Department portable or removable storage device that contains data classified as Level 1 and which is not encrypted.

Level 2 – Medium

Medium security incidents affect the availability of services or data. The following are some examples of medium security incidents:

- Loss, theft, or unauthorized disclosure of electronically stored data classified as Level 2 or Level 3 electronically stored data which is not encrypted and which does not include personally identifiable information;
- Loss, theft, or unauthorized disclosure of physical information which contains data classified as Level 2 or Level 3 and which does not include personally identifiable information; and
- Any security incident which allows an intruder access at a level less than privileged, which could lead to further opportunity to obtain greater access whether electronic or physical.

Level 3 – Severe

Severe security incidents affect critical information systems or data. The following are some examples of severe security incidents:

- Virus, worm, or other malicious code propagation without user action;
- A security incident which allows an intruder to gain privileged access (admin/root) to a system;
- A security incident which allows an intruder to gain unauthorized physical access to a secured facility;
- The physical or electronic compromise of confidentiality, integrity, availability of data or the integrity or availability of processing resources;
- Loss, theft, or unauthorized access and/or dissemination of personally identifiable information whether physical or electronic;
- Loss, theft, or unauthorized disclosure of physical information (manual records) classified as Level 3 or Level 4;
- Loss, theft, or unauthorized disclosure of electronic data classified as Level 3 or Level 4 which is not encrypted.

Oregon Department of Justice
Security Incident Response Communications Plan
(Revised xx/xx/xxxx)

Security Incident Communications will be based upon the priority assigned to the security incident. A priority will be assigned to each security incident upon examination and review of the event. Loss, theft or unauthorized disclosure of personally identifiable information will follow the communication requirements as described in the Oregon Identify Theft Protection Act.

Only communications authorized by the Security Incident Response Team (SIRT) and Department Management may communicate information about a security incident. Communicating information haphazardly about a security incident could further increase the risk to the Department and to the State of Oregon.

Priority 1 (Low) security incidents require the Security Incident Response Team to create an e-mail which will be sent to the manager or to other designated customers of the affected areas as required. In the event that the Department's e-mail system is unavailable, the information will be dispersed by telephone. The communication will state:

- What non-critical device/system is affected;
- That the incident is being worked on; and
- Estimated time to resolution.

Priority 2 (Medium) security incidents require the Security Incident Response Team to create an e-mail which will be sent to the employee's supervisor by the Customer Services Center and to other designated customers as required. In the event that the Department's e-mail system is unavailable, the information will be dispersed by telephone. The communication will state:

- What the security incident is;
- What workstation, device, laptop, etc., has been affected;
- That the incident is being worked on; and
- Estimated time to resolution.

Priority 3 (High) security incidents require the Security Incident Response Team to create an e-mail for dispersion by the Customer Service Center that will be delivered to all customers affected. In addition, the Customer Service Center will notify the main point of contact for each Division affected by telephone. The communication will state:

- What the security incident is;
- What systems or availability of systems the incident has affected;
- That the incident is being worked on;
- Estimated time to resolution;
- Updates will be forthcoming; and
- State any prescribed course of action the customers must take until the incident is resolved.

Oregon Department of Justice
Security Incident Response Report Guidelines
(Revised xx/xx/xxxx)

Security Incident Response Team Reports are required on all security incidents that the SIRT responds to. The following information is provided as a guideline for developing detailed security incident response reports. At the conclusion of each report, there must be a recommended course of action that specifies what should be done to prevent the future reoccurrence of the security incident.

Preparation

- Were detection capabilities in place that discovered this incident?
- Were security controls in place to prevent the security incident?
- What conditions allowed the security incident to happen?
- What could have prevented this security incident?
- Was this security incident reported promptly?

Detection

- How soon after this security incident occurred was it detected?
- What could have been done to detect this earlier?
- Was the Security Incident Response Policy followed?
- Did the SIRT respond in a prompt manner?
- Were the required parties informed of the security incident?

Containment

- How quickly was the security incident contained?
- What was done to contain the security incident?
- If services were disrupted to our customers to contain this security incident, was the CIO notified?
- If services were disrupted to our customers to contain this event, was customer management notified?
- Could changes be made to the environment that would have made containing the security incident easier or faster?
- Were all containment actions documented?
- Was criminal activity involved?
 - Was appropriate action taken or sought?
 - Criminal intent?
 - Was notification completed as required by law or statute?

Corrective Action

- Was the security incident corrected?
- Was data recovered if involved, and was any data permanently lost or compromised?
- How were corrective actions prioritized if the security incident covered multiple devices, systems, or locations?
- Were the necessary tools readily available to support the corrective actions taken?
- Did the staff have the necessary training to determine and implement the necessary corrective actions to remedy the security incident?

Incident Review

- What could be done to prevent this security incident from reoccurring?
- What security controls could be put in place to protect or detect against security incidents of this nature?
- What training or education could be implemented to solve or prevent security incidents of this type?
- What was learned from this security incident?

**Oregon Department of Justice
Security Incident Response Team Members**

The Security Incident Response Team is comprised of the following positions:

- Chief Information Officer
- IS Management
- Security Coordinator
- Network Security Team Lead
- Network Services Team Lead
- Application Development Team Lead
- Mainframe Team Lead (when applicable)
- Desktop Services Team Lead
- Customer Service Center Team Lead
- Legal Division Representative (one per division)
- DCS Representative
- ESO Representative (when required)
- SDC Representative (when required)

DRAFT

**Oregon Department of Justice
Security Incident Response Form**

(1) Contact Information (person reporting the Incident)

Name:	Division:	Section:	Phone number:
--------------	------------------	-----------------	----------------------

(2) Security Incident Details

Date and Time Reported:	Date and Time Discovered:	HelpStar:
--------------------------------	----------------------------------	------------------

Incident Category: () External () Internal () Physical	Incident Classification Level: () Level 3 – Severe () Level 2 – Medium () Level 1 - Low	Source (IP if known):
---	--	------------------------------

Incident Description:

Resources Affected:

(3) Actions Taken:

(4) Incident Assessment

Technical Impact of the Incident:

Information/Data lost:

Business Impact of the Incident:

Severity of Incident:	Loss of business hours:	Loss of IT hours:
------------------------------	--------------------------------	--------------------------

(5) Incident Categorization (Check which apply)

<input type="checkbox"/>	Virus or Worm	<input type="checkbox"/>	Unauthorized Access	<input type="checkbox"/>	DoS Attack
<input type="checkbox"/>	Compromised User Account	<input type="checkbox"/>	Policy Violation (e-mail)	<input type="checkbox"/>	Policy Violation (Internet)
<input type="checkbox"/>	Loss of Laptop	<input type="checkbox"/>	Loss of Portable Device	<input type="checkbox"/>	Loss of data
<input type="checkbox"/>	Other (Specify):	<input type="checkbox"/>	Loss of PII	<input type="checkbox"/>	Physical Intrusion

(6) Shared with ESO? (Yes or No):

(7) Risk Management notified? (Yes or No):

(8) Was Personally Identifiable Information Involved (Yes or No):