



**DEPARTMENT OF CORRECTIONS  
Information Systems**



<b>Title:</b>	<b>Information Security Incident Response</b>	<b>DOC Policy: 60.1.6</b>
<b>Effective:</b>	<b>3/1/12</b>	<b>Supersedes: 6/1/09</b>
<b>Applicability: All DOC employees, contractors, and volunteers</b>		
<b>Directives Cross-Reference:</b>		
<ul style="list-style-type: none"> <li><b>Policy: Code of Conduct – 20.1.3</b></li> <li><b>Employee Assigned Assets – 30.2.3</b></li> <li><b>Keys and Locks, Policy – 40.1.2</b></li> <li><b>Operations Division Peer Audit – 40.1.4</b></li> <li><b>Unusual Incident Reporting Process – 40.1.6</b></li> <li><b>Acceptable Use of Electronic Information Systems – 60.1.1</b></li> <li><b>Electronic Mail, Internet Usage and Computer Investigations – 60.1.2</b></li> <li><b>Information Technology Asset Management – 60.1.3</b></li> <li><b>Information Security – 60.1.4</b></li> <li><b>Information Security Awareness– 60.1.5</b></li> </ul>		
<b>Rule: Network Information System Access and Security – Div 005</b>		
<b>Attachments: Information Security Incident Report (CD 1581)</b>		
<b>Information Security Incident-Supervisor Checklist (CD 1580)</b>		

**I. PURPOSE**

The purpose of this policy is to create effective responses to information security incidents that affect the availability, integrity, or confidentiality of the Department's information assets. The policy defines the structure for incident response, roles and responsibilities, and the requirements for reporting incidents.

**II. DEFINITIONS**

- A. Availability: The reliability and accessibility of information assets and resources to authorized individuals in a timely manner.
- B. Confidentiality: A security principle that works to ensure that information is not disclosed to unauthorized subjects.
- C. Incident: A single or a series of unwanted or unexpected information security events that result in harm, or pose a significant threat of harm to information assets, an agency, or third party and require non-routine preventative or corrective action.
- D. Incident Response Plan: Written document that states the approach to addressing and managing incidents.
- E. Incident Response Policy: Written document that defines organizational structure for incident response, defines roles and responsibilities, and lists the requirements for respond to and reporting incidents.

- F. Incident Response Procedures: Written document(s) of the series of steps taken when responding to incidents.
- G. Incident Response Program: The combination of DOC incident response policy, plan, and procedures into an operational program.
- H. Information Asset: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, including electronic, paper, and verbal communication that has value to the agency.
- I. 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.
- J. Information Security Event: An observable, measureable occurrence in respect to an information asset that is a deviation from normal operations.
- K. Integrity: A security principle that makes sure that information and systems are not modified maliciously or accidentally.
- L. Restricted and Critical Information: Any information receiving a data classification level of 3 or 4.
- M. Risk: The likelihood of a threat agent taking advantage of vulnerability and the resulting business impact.

### **III. POLICY**

#### **A. Information Security Incident Response Program**

The department has created an incident response program to respond to electronic, paper, or verbal information security incidents. The program consists of the DOC Information Security Incident Response Plan (IRP), staff development, and ongoing review. All employees must follow the DOC IRP whenever an information security incident is suspected, or actually occurs.

#### **B. Reporting Information Security Incidents**

1. Staff must immediately report incidents and gather data surrounding incidents that involve information security, along with assessments of vulnerability and risk, to the DOC Information Security Officer (ISO).
2. Timely reporting enables prompt corrective action and allows for thorough information gathering and reporting.
3. The ISO and OIM shall share information security incidents with the DOC Chief Information Officer (CIO), DOC Director, and the State Incident Response Team (SIRT) within 24 hours of occurrence. The ISO will communicate with the SIRT to coordinate, investigate, and respond to an information security incident when needed. If the incident involved a breach of credit card information, the ISO will inform the Oregon State Treasury within 24 hours.

#### **C. Information Security Incident Response Plan**

DOC has developed an Information Security Incident Response Plan (IRP) to respond to agency incidents. The plan includes roles, responsibilities, processes, and procedures for handling information security incidents.

**D. Reportable information security incidents must meet all four of the criterion below:**

1. Involves information security (see definitions);
2. Is unwanted, unexpected, or accidental;
3. Shows harm, intent to harm, or significant threat of harm; and
4. Response requires non-routine action.
5. Reporting is mandatory for any information security incident that meets all these criteria. Reporting by DOC staff is recommended for any information security incident meeting at least one, but fewer than all four criteria. The DOC Information Security Incident Response Plan provides detailed reporting requirements.

**E. Examples of reportable and non-reportable information security incidents**

1. Examples of non-reportable information security incidents:
  - a. Criminal violations with no information security component, such as theft of a car containing no department assets (no information security involved)
  - b. Increased web site activity, due to popularity, that leads to site unavailability (not unwanted or unexpected)
  - c. Briefcase containing public disclosable information is lost (no harm, no intent to harm, or not significant threat of harm)
  - d. Computer virus is detected on a workstation that is successfully contained by anti-virus software (no non-routine action required)
  - e. SPOTS card fraud/losses (routine process already established with U.S. Bank)
2. Examples of reportable information security incidents include the following:
  - a. Any information security incident relevant to the Oregon Consumer Identify Theft Protection Act
  - b. Lost or stolen documents or IT Equipment containing restricted or critical information
  - c. Conversation containing sensitive information overheard by unauthorized person who discloses the information to the public
  - d. A virus or worm that has become widespread in the Department

- e. Website defaced
- f. Unauthorized access to information
- g. Any kind of sabotage that effects information
- h. Denial of service attacks
- i. Loss of building keys or key cards

#### **IV. IMPLEMENTATION**

This policy will be adopted immediately without further modification.

Certified: \_\_\_\_\_  
Birdie Worley, Rules Coordinator

Approved: \_\_\_\_\_  
Mitch Morrow, Deputy Director