



**DEPARTMENT OF CORRECTIONS  
Information Systems**



<b>Title:</b>	<b>Information Security</b>	<b>DOC Policy: 60.1.4</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>		
<b>Policy: Acceptable Use of Electronic Information Systems-60.1.1</b> <b>Information Security Awareness-60.1.5</b> <b>Information Security Incident Response-60.1.6</b>		
<b>Rule: Network Information System Access and Security – Div 005</b>		
<b>Attachments: None</b>		

**I. PURPOSE**

- A. It is the policy of the State of Oregon to ensure the privacy, integrity, and availability of information assets entrusted to the State by the citizens. This will be accomplished by protecting those assets from unauthorized access, modification, destruction, or disclosure and to ensure their physical security.
- B. The Oregon Department of Corrections (DOC) will establish an Information Security Program that complies with State policies and other federal and state regulations. The Information Security Program will clearly state organization-wide objectives, clarify and assign responsibilities, develop and implement security policies and practices, and provide a framework for enforcement. DOC has a responsibility to ensure that all information held by the department, is appropriately secure.
- C. The purpose of the DOC Information Security Program is three-fold:
  - 1. Establish policies and procedures and provide standard tools to secure ODOC data in compliance with state and federal security requirements, using minimum levels of industry standards;
  - 2. Support the ODOC mission through practice of good stewardship of information assets; and
  - 3. Develop and implement an Information Security Plan that provides clear guidance and vision to a consistent organizational approach to Information security Management.

**II. POLICY**

- A. Information Security Program
  - 1. Organization-wide objective: DOC will secure its information assets to maintain confidentiality, integrity, and availability of those assets.

2. DOC will establish an Information Security Program. The program will provide risk assessment of DOC information assets, appropriate and effective policies for adequate protection, and assurance that the security policies are effectively applied. The Information Security Program will clearly state organization-wide objectives, clarify and assign responsibilities, develop and implement security policies and practices, and provide a framework for enforcement.
3. The Information Security Program will address, at a minimum, information asset classification, access control, personnel security, physical and environmental security, operational security, systems security, and business continuity management.
4. Security policies and program will be reviewed at least annually to accommodate organizational changes.

B. Scope:

1. This policy applies to all types of information generated, used, or held by DOC that are used within the scope of DOC business processes. This policy covers information assets in all formats, including electronic, cardholder data, magnetic, paper, or other.
2. All individuals who have been granted access to DOC information or information systems, including but not limited to full- and part-time employees, contractors, temporary workers, those employed by others to perform DOC work, and others granted access are covered by this policy and shall comply with this and associated policies, procedures and guidelines.

C. Compliance Failure to comply with this policy and associated policies, standards, guidelines, and procedures may result in disciplinary actions up to and including dismissal from state service for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

D. Responsibilities: Individuals, groups, or organizations identified in the scope of this policy are accountable for one or more of the following levels of responsibility when using DOC information assets:

1. All information generated, acquired by or on behalf of, or held by DOC within its systems of operation is the property of the Oregon Department of Corrections, unless otherwise stated in a contractual agreement. DOC has a responsibility to ensure that all information held by the department is appropriately classified and secure.
2. The DOC Director is responsible and accountable for the information assets held by the agency. The Director is responsible for establishing policies and procedures governing:
  - a. The integrity of information assets.
  - b. The authorization of access to those assets.

- c. Compliance with legal requirements for information privacy.
  - d. Implementation of a security program within the Oregon Department of Corrections.
3. The DOC Information Security Officer is responsible for:
- a. Development and maintenance of the DOC Information Security Program.
  - b. Development of a security strategy that aligns with business and technology objectives.
  - c. Creation and formalization of a program for implementing the security policies.
  - d. Development of methodologies consistent with best business practices designed to ensure repeatable outcomes.
  - e. Development of a process to keep the program and policies current as changes to technology and business occur.
  - f. Establishment of procedures for appropriate actions when information security policies have been violated.
  - g. Development of measurable outcomes that assess the success of the security program.
4. All DOC employees, contractors, volunteers and individuals who have access, use or hold DOC information assets, share the responsibility for the security and integrity of the information assets. They are responsible for:
- a. Compliance with all information security policies, procedures, rules and plans.
  - b. Report information security events and incidents in accordance with DOC policy on **Information Security Incident Response**, 60.1.6.
5. Information users (users) are the individuals, groups, or organizations authorized by DOC to access information assets. Users are responsible for:
- a. Using the information only for its intended purposes. If the user has a question about appropriate use or the intended purpose of information, the user must check with the appropriate supervisor or manager for clarification.
  - b. Maintaining the confidentiality, integrity, and availability of the information.
  - c. Report information security events and incidents in accordance with DOC policy on **Information Security Incident Response**, 60.1.6.

### III. IMPLEMENTATION

This policy will be adopted immediately without further modification.

Certified: Signature on file  
Birdie Worley, Rules Coordinator

Approved: Signature on file  
Mitch Morrow, Deputy Director