	DEPARTMENT OF CORRECTIONS **Information Systems**	
Title:	**Information Security Program**	**DOC Policy: 60.6.1**
Effective:	**7/19/23**	**Supersedes: 8/5/22**
Applicability: All DOC employees, contractors, and volunteers		
Directives Cross-Reference: **Information Security Training and Awareness Program – (DOC) 60.6.2** **State Information Security – (DAS rule) OAR 125-800** **Cyber and Information Security – (DAS policy) 107-004-052** **Oregon Statewide Information and Cyber Security Standards**		
Attachments: None		

I. PURPOSE

The purpose of this policy is to ensure the confidentiality, integrity, and availability of information assets through the development and continued review of an Information Security Program within the Department of Corrections (DOC).

This policy applies to all DOC employees, contractors, volunteers, third party and external entities that access department information technology for information classification, gathering, creating, editing, transmitting, viewing, or destruction of information assets belonging to DOC. See also the department's policy on Acceptable Use of Oregon Department of Corrections Information Technology (DOC policy 60.1.1).

II. DEFINITIONS

A. Availability: Ensuring timely and reliable access to and use of information.

B. Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

C. Department Computing Devices: All electronic information devices, interconnections, and technical information of the department. Examples of systems include, but are not limited to:

1. Computers, printers, copiers, recorders, transmitters, data telecommunications connections and any similar connected devices.
2. All portable devices such as cell phones, smart phones, tablets, MP3 players, and any other devices within the department.
3. Networking devices includes routers, switches, VPN concentrators, or any device interconnecting networks.

4. Large scale information systems which provide services to the department such as logon access, file servers, data warehousing, web access, web hosting, and mail and instant message services.
5. Applications such as Corrections Information System (CIS), Integrated Supervision Information Systems (ISIS), DOC 400, or any other systems accessed by or through these systems or systems devices. Methods include, but are not limited to, the Internet, Internet Service Providers (ISP) and DOC hosted connections.

D. Information: Data or knowledge that is transmitted, analyzed, edited, or reproduced in department systems by electronic, printed, written, verbal, or media transmission means. Examples include, but are not limited to:

1. Documents, reports, statistics, files, records, and logs compiled or stored on DOC computing devices or applications.
2. E-mails or messaging system conversations and their attachments.
3. Audio and video files.
4. Images such as graphics, pictures, and photographs.
5. Programs (such as CIS, DOC400, ISIS, WebLEDS, etc.), software, and macros.
6. Text and data.

E. Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

F. Integrity: Guarding against improper information, modification, or destruction, and includes ensuring information non-repudiation and authenticity.

III. POLICY

A. Information Security Program

1. The department will establish an Information Security program that satisfies the following criteria:

2. Clearly states the organization-wide objectives, clarifies and assigns responsibilities, develops and implements simple, yet effective policies and procedures, and provides a framework for enforcement thereof.

3. Complies with federal and state laws, rules, policies, regulations, and requirements. See also Department of Administrative Services (DAS) policy on State Information Security (107-004-052) and DAS rule on State Information Security (OAR 125-800).

4. Guarantees the confidentiality, integrity, and availability of information assets entrusted to the department. These requirements will be accomplished by:

    a. A well-documented information security program.

b. Maintaining minimum industry standards, while striving for industry best practices. See Oregon Statewide Information and Cyber Security Standards.

c. Implementing appropriate administrative, physical, and technical controls equal to the asset's classification level.

5. Annual review of all federal and state laws, administrative rules, department policies, procedures, and compliance requirements for relevancy and accuracy.

6. Create or procure appropriate training in regard to legal, business, and information assets, as well as technology processes and procedures that the department uses in its Information Security Program. See also the department's policy on Information Security Training and Awareness Program (DOC policy 60.6.2).

B. **Asset Classification**

1. The process of asset classification is to identify the proper level of security for information under the control of DOC. This is to ensure that assets are not accidentally or willfully disclosed, altered, or destroyed.

2. The creator of the information asset is the responsible party to assign the classification level.

3. To evaluate the appropriate level of protections placed on assets the department will use a risk-based approach

4. To continually assist the DOC Records Office in the determination of information retention periods.

C. **Assessments**

1. The department must conduct regularly scheduled information security assessments and testing to ensure the program's viability.

2. Assessments completed by outside contracted resources acquired by Cyber Security Services, or another department office will constitute the requirements being met.

3. Assessments can be conducted without warning or notification to ensure continued and constant compliance with federal, state, and department laws, rules, policies, procedures, and standards (Oregon Statewide Information and Cyber Security Standards).

IV. IMPLEMENTATION

This policy will be adopted immediately without further modification.

Certified: ___signature on file_____
Julie Vaughn, Rules Coordinator

Approved: ___signature on file_____
Heidi Steward, Acting Director