DEPARTMENT OF CORRECTIONS
Information Technology Services

Title:	**Information Security Training and Awareness Program**	**DOC Policy: 60.6.2**
Effective:	**7/19/23**	**Supersedes: 8/5/22**
Applicability:	**All DOC employees, contractors, and volunteers**	
Directives Cross-Reference:	**Professional Development Training – (DOC) 20.7.1** **Acceptable Use of Oregon Department of Corrections Information Technology – (DOC) 60.1.1**	
Attachments: None		

I. PURPOSE

The purpose of this policy is to educate users on their responsibility to help protect the confidentiality, integrity, and availability of the department's information assets and to ensure that all personnel are trained on relevant rules, regulations, and best practices regarding their role in the department's cybersecurity posture. This policy applies to all Department of Corrections (DOC) employees, contractors, and volunteers that use DOC computing devices and have access to all levels of information assets created, gathered, modified, stored, transmitted, or used within the department, regardless of whether it is written, verbal, or electronic in format.

II. DEFINITIONS

A. Awareness: A learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure.

B. 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.

C. Training: Informing personnel of their roles and responsibilities within a particular Information Technology (IT) plan and teaching skills related to those roles and responsibilities.

III. POLICY

A. Basic Training Requirements

1. DOC shall provide ongoing information security training and an awareness campaign to all staff, contractors, and volunteers that use department resources.

2. The DOC Information Security Officer (ISO) will oversee the department information security training and awareness program, including its creation, implementation, testing, and revision, when necessary, prior to distribution.

3. DOC ISO or designee will work with DOC Professional Development Unit to coordinate, monitor, track and report the completion of department information security training and awareness. Additionally, incomplete or outdated training will be reported to appropriate managers. See also the department's policy on Professional Development Training (DOC policy 20.7.1).

4. Current versions of security policies and procedures will be included in the information security training and awareness program.

5. Each manager is responsible for ensuring that department employees, contractors, and volunteers complete mandatory information security training prior to accessing department resources.

6. All department employees, contractors, and volunteers will complete information security training within the first 30 days of beginning work.

7. Continual information security training will be completed on an annual basis.

8. Additional security training will be required in response to security threats and incidents in compliance with legislation, regulations, and industry standards where awareness is necessary.

9. Failure to complete required training to access department or other agency resources could lead to revocation of access until required training has been accomplished.

10. All department employees, contractors, and volunteers are required to acknowledge that they have read, understand, and accept all DOC security policies and procedures, including the training. See the department's policy on Acceptable Use of Oregon Department of Corrections Information Technology (DOC policy 60.1.1).

B. Specialized Training Requirements

1. The department understands that general information security training is not adequate for staff that have specialized positions or skillsets.

2. The DOC ISO or designee will make specialized information security training requirements available to those specialized staff positions needing additional training. This training may include, but is not limited to:

    a. Criminal Justice Information System (CJIS)

    b. Law Enforcement Data System (LEDS)

    c. Health Insurance Portability and Accountability Act (HIPAA)

    d. Payment Card Information-Data Security Standards (PCI-DSS)

    e. Open Web Application Security Project (OWASP)

f. Federal Education Rights and Privacy Act (FERPA)

g. Federal Information Systems Modernization Act (FISMA)

h. Oregon Consumer Information Protection Act (OCIPA)

3. DOC ISO or designee will coordinate, monitor, track, and report the completion of department information security training and awareness. Additionally, incomplete or outdated training will be reported to appropriate managers.

4. Failure to complete required training to access department or other agency resources could lead to revocation of access until required training has been accomplished.

C. Awareness Program

1. DOC shall provide an ongoing information security awareness campaign to all staff, contractors, and volunteers that use department resources.

2. Information security awareness may be delivered through multiple mediums, discussing information security topics.

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