DEPARTMENT OF CORRECTIONS
Information Systems

Title:	**Information Security Incident Response**	**DOC Policy: 60.6.3**
Effective:	**7/19/23**	**Supersedes: 8/5/22**
Applicability:	**All DOC employees, contractors, and volunteers**	
Directives Cross-Reference: **Cyber and Information Security Incident Response – (DAS) 107-004-120** **Information Security Program – (DOC) 60.6.1** **State of Oregon Information Security Incident Response Plan**		
Attachments: None		

I. PURPOSE

The purpose of this policy is to protect the confidentiality, integrity, and availability of information assets in the event of a security incident consisting of, but not limited to, loss, theft, malware, or threat actors through information security processes within the Department of Corrections (DOC).

This policy applies to all DOC employees, contractors, and volunteers that use department information technology for the classification, creation, destruction, editing, transmitting, gathering, or viewing of DOC information assets, regardless of location.

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. Computing Device: A device that can perform substantial computations, including numerous arithmetic operations and logic operations without human intervention. A computing device can consist of a standalone unit or several interconnected units. It can also be a device that provides a specific set of functions, such as a phone or a personal organizer, or more general functions such as a laptop or desktop computer.

D. Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

E. Information: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms.

F. 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.

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

H. Risk: A measure of the extent to which an entity or individual is threatened by a potential circumstance or event, and typically is a function of the adverse impact that would arise if the circumstance or event occurs and the likelihood of occurrence.

I. Security Event: An observable, measurable occurrence involving an information asset that is relevant to security operations.

III. POLICY

A. Information Security Incident Response (ISIR) Program

1. The department will establish an information security incident response program. This program must contain the department ISIR policy, ISIR plan, and ISIR procedures. See also the department's policy on Information Security Program (DOC policy 60.6.1).

2. All documents must be annually reviewed for applicability.

3. The DOC Information Security Officer (ISO) or their designee will create or procure appropriate incident response training that is in line with legal, regulatory, business, or technology processes and procedures that the department utilizes as part of its information security program.

4. If the DOC ISO or their designee determines an incident rises to the level of emergency status, the agency emergency response policy shall take precedence and the incident response plan shall be utilized in the after-action process.

B. Information Security Incident Response Plan

1. DOC ISO will establish an ISIR plan to assist all departments in the event of an incident. The plan must do or include the following (see also State of Oregon Information Security Incident Response Plan):

   a. Clearly states the organization-wide objectives, clarifies assigned roles and responsibilities, and develops and implements simple effective procedures.
   b. Defines incident classifications. Incident classifications will be dependent on criticality of system, type of activity, information assets value, number of people or functions impacted, ability to be contained, political sensitivity, and press involvement or publicity.
   c. Must comply with federal and state laws, rules, policies, regulations, and compliance requirements.
   d. Annual review of all federal and state laws, administrative rules, department policies, procedures, and compliance requirements for relevancy and currency.

2. The ISIR plan must be reviewed and tested annually for functionality and applicability.

C. Information Security Incident Response Procedures

1. DOC ISO will establish and provide staff with ISIR procedures. These documents will assist all departments with step-by-step instructions on how to report, react, and remediate an information security incident. See also Department of Administrative Services (DAS) policy on Cyber and Information Security Incident Response (DAS policy 107-004-120).

2. The ISIR plan shall be reviewed and tested annually for functionality and applicability.

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