ENTERPRISE information services

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES STATEWIDE POLICY	**NUMBER** 107-004-120	**SUPERSEDES** Policy # 107-004-120 | 11/10/2008
	EFFECTIVE DATE November 16, 2020	**PAGE NUMBER** Pages 1 of 5
	DATE OF LAST REVIEW November 16, 2020	
Division **Enterprise Information Services (State CIO)**	**REFERENCE** ORS 276A.300, 276A.303, 276A.306, 276A.323, 276A.326, 276A.329, 276A.332, 276A.335 OAR 125-800	
Policy Owner Cyber Security Services		
SUBJECT Cyber and Information Security Incident Response	**APPROVED SIGNATURE** Terrence Woods, State Chief Information Officer *(Signature on file with DAS Business Services)*	

PURPOSE

This policy defines Oregon state government's approach to cyber and information security incident response. Effective incident response helps protect the availability, integrity and confidentiality of state information assets.

APPLICABILITY

This policy applies to all state agencies as defined in ORS 276A.230, and includes any board, commission, department, division or office within the Oregon Executive Branch. The following agencies and boards are excluded:

- Secretary of State.
- State Treasurer.
- The Attorney General, but only with respect to its authority under ORS 276A.303 over information systems security in the Department of Justice.
- Oregon State Lottery.
- State Board of Higher Education or any public university listed in ORS 352.002.

FORMS/EXHIBITS/INSTRUCTIONS

The State Information Security Incident Response Plan further details roles and processes for the state's response to cyber and information security incidents.

An Agency Incident Response Plan Template is available to assist agencies in establishing or updating their incident response plan.

These documents and other incident response resources are available at: https://www.oregon.gov/das/OSCIO/Pages/SecurityResponse.aspx.

DEFINITIONS

Asset: Anything that has value to an organization.

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

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

Incident Response Plan: Written document that states the approach to addressing and managing incidents.

Incident Response Policy: Written document that defines organizational structure for incident response, defines roles and responsibilities, and lists the requirements for responding to and reporting incidents.

Incident Response Procedures: Written document(s) detailing the steps taken when responding to incidents.

Information: Any communication or representation of knowledge in any medium or form. Examples include but are not limited to:

- Documents, reports, statistics, files, and records, compiled or stored in digital or physical form.
- Emails or messaging system conversations and their attachments.
- Audio and video files.
- Images, graphics, pictures and photographs.
- Programs, software and macros.
- Spoken conversations.

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.

Integrity: Guarding against improper information modification or destruction, which ensures information non-repudiation and authenticity.

Risk: A measure of the extent to which an organization is threatened by a potential circumstance or event, which takes into account the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence.

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

Security Incident: A single or series of unwanted or unexpected security events (refer to definition of "security event") that results in harm, or poses a significant threat of harm, to information assets, an agency, or third party and requires non-routine preventive or corrective action.

GENERAL INFORMATION

(1) General Roles and Responsibilities

Responsibility for incident response is shared among Enterprise Information Services (EIS), Cyber Security Services (CSS) and agencies to ensure that state response efforts are adequate, uniform, and coordinated, regardless of incident size or complexity.

(a) **Enterprise Information Services – Cyber Security Services:**

CSS manages the state's response to incidents including those involving an actual or suspected breach under the Oregon Consumer Information Protection Act (ORS 646A.600 et seq.). Depending upon the incident scope and impact, and agency capabilities, CSS may either directly manage the incident or coordinate with the affected agency on the incident response. The CSS's role may change during the incident.

CSS Security Operations Center (SOC) will collect, classify, and catalog all reported information security incidents and assess incident scope and impact. CSS SOC will respond to information security incidents that potentially impact multiple agencies or which pose a significant risk to the state. CSS SOC manages inter-agency incident response resources and communications for incidents that impact multiple agencies. In addition, CSS maintains expertise and capabilities to assist state agencies with incident response.

CSS will establish enterprise policy, standards, and guidelines for statewide and agency-level cyber and information incident response. CSS will develop and maintain the State Information Security Incident Response Plan to define processes for incident response preparation; detection and analysis; containment, eradication and recovery; and post-incident analysis. CSS may also develop supporting procedures and processes. CSS also leads enterprise training, exercises, and other activities to test, evaluate, and improve the incident response program.

The State Chief Information Security Officer develops partnerships and engages with the Oregon Cybersecurity Advisory Council, regional and local governments, other state governments, the federal government, law enforcement organizations, and private sector entities to prepare for, respond to and recover from incidents.

(b) **Agencies:**

Agencies are responsible for reporting incidents to CSS SOC, per "Reporting Information Security Incidents" below, and for taking steps necessary to respond to an incident, in coordination with or at the direction of the CSS SOC.

Each agency must maintain the capability to respond to information security incidents involving information in any form. Agencies may establish this capability by using internal or a combination of internal and external resources, but at a minimum agencies must maintain:

- An incident response plan.
- Processes and procedures for implementing this incident response plan.
- A point of contact to interface with CSS SOC.

State agencies may, based on their individual business needs or legal or regulatory requirements, exceed the requirements outlined in this policy but must meet these minimum requirements.

Agencies must maintain an internal incident response plan that details agency processes and responsibilities, including how the agency will support CSS-led incident response efforts. The agency plan must align with the State Information Security Incident Response Plan. Agency incident response plans must identify:

- Incident response roles and responsibilities.
- Resources and procedures for incident management across the following activities:
    - Preparation.
    - Detection and Analysis.
    - Containment, Eradication and Recovery.
    - Post-Incident Activity.
    - Communications with internal and external stakeholders.
    - Notification of CSS SOC upon incident determination.
- Procedures for managing incidents involving regulated information, including documenting notification requirements and processes.

- Awareness training regarding information security incident responsibilities, incident identification and reporting.
- Training for designated responders specific to their role within an incident.
- Processes for testing and updating the plan.

Agencies must review incident response plans annually and update plans to address system and organizational changes; lessons learned during plan implementation, testing or execution; and changes in enterprise policy, standards and guidance.

Agencies must provide incident response plans to CSS SOC for review.

(2) **Reporting Information Security Incidents**

Each agency must report information security incidents to CSS SOC no later than 24 hours after discovery via the CSS SOC Hotline, 503-378-5930. In some cases, it may not be feasible to have complete and validated information prior to reporting. Agencies should provide all available information at the time of notification and report updated information as it becomes available.

If unsure whether a situation is an incident, agencies should consult with CSS SOC to determine if an incident has occurred. Agencies should err on the side of caution and report all *suspected* incidents to CSS SOC.

State agencies are also required to report incidents to the Legislative Fiscal Office (per ORS 276A.306), and to make any other notifications required by law or regulation.

Reportable incidents must meet all four of the following criteria (for examples, refer to “Guidelines” below):

- Involves information security.
- Is unwanted or unexpected.
- Shows harm, intent to harm or significant threat of harm.
- Requires a non-routine response.

All users who are provided authorized access to agency information or systems are responsible for promptly reporting suspected or actual security incidents to their agency points of contact.

Upon identification of an incident, the agency must immediately initiate its incident response plan and designate a point of contact to communicate information security incidents to CSS. The agency point of contact will work with CSS to establish the method of reporting. CSS will communicate with the agency point of contact to coordinate, investigate and respond to the incident, as needed. The agency must support CSS in its responses, including but not limited to, providing the necessary resources, providing all requested information and taking actions as directed by CSS.

(3) **Incident Categorization**

CSS will categorize incidents as described in the *State Information Security Incident Response Plan*. CSS has ultimate authority to determine an incident has occurred and to categorize incidents, and may reclassify and escalate incidents as conditions change. CSS may require agencies to take action based upon the incident categorization.

GUIDELINES

An incident involves a single or series of unwanted or unexpected information security events that results in harm, or poses a significant threat of harm, to information assets, an agency, or third party and requires non-routine preventive or corrective action. Incidents may take various forms – for example, some incidents involve a breach of personal information – and can stem from various causes. The lists below provide examples of reportable information security incidents, along with examples of events that agencies do not need to report to CSS SOC. These lists are meant to guide agencies, but are not comprehensive.

- Reportable incidents include, but are not limited to, the following:
  a. Any incident relevant to regulated data, including the Oregon Consumer Identity Protection Act; breaches of personal information are a type of incident.
  b. Malware that has become widespread.
  c. Successful phishing attempt.
  d. Denial of service attacks.
  e. Lost or stolen documents or information assets (e.g., laptop, thumb drive, etc.) containing sensitive or potentially sensitive information.
  f. Conversation containing Level 3 or Level 4 information overhead by an unauthorized person who discloses the information to the public.
  g. Website defaced.
  h. Unauthorized access to information.
  i. Any kind of sabotage that affects information or information systems.

- Non-reportable events that do not qualify as incidents include the following:
  a. Criminal violations with no information security component, such as car theft.
  b. Increased website activity that leads to the site becoming unavailable (activity is not unwanted or unexpected – e.g. due to popularity).
  c. Documents lost, where there is no harm, no intent to harm, or no significant risk of harm (e.g., briefcase containing publicly disclosable documents).
  d. Computer virus detected on a workstation that is successfully contained by anti-virus software (i.e., no non-routine action is required).