# Introduction

ORS 276A.300 directs the Office of the State Chief Information Officer and agencies to collaboratively develop and implement policies for responding to incidents that involve the security of information. The statewide Information Security Incident Response Policy 107-004-120 further requires agencies to maintain an incident response capability. The statute also requires reporting incidents and plans to the Cyber Security Services. The Oregon Consumer Identity Theft Act (ORS 646A.600) requires agencies to take specific actions in cases where compromise of personally identifiable information has occurred. This plan addresses these requirements.

An incident response plan brings together and organizes the resources for dealing with any event that harms or threatens the security of information assets. Such an event may be a malicious code attack, an unauthorized access to information or systems, the unauthorized use of services, a denial of service attack, or a hoax. The goal is to facilitate quick and efficient response to incidents, and to limit their impact while protecting the state’s information assets. The plan defines roles and responsibilities, documents the steps necessary for effectively and efficiently managing an information security incident, and defines channels of communication. The plan also prescribes the education needed to achieve these objectives.

# 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, or to [ESO.SOC@oregon.gov](mailto:ESO.SOC@oregon.gov). 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.

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:

* Any incident relevant to regulated data, including the Oregon Consumer Identity Protection Act;   
  breaches of personal information are a type of incident.
* Malware that has become widespread.
* Successful phishing attempt.
* Denial of service attacks.
* Lost or stolen documents or information assets (e.g., laptop, thumb drive, etc.) containing   
  sensitive or potentially sensitive information.
* Conversation containing Level 3 or Level 4 information overhead by an unauthorized person   
  who discloses the information to the public.
* Website defaced.
* Unauthorized access to information.
* Any kind of sabotage that affects information or information systems.

Non-reportable events that do not qualify as incidents include the following:

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

# Roles and Responsibilities

**[[Agency]]**

Responsible for

* reporting incidents, or possible incidents, to Cyber Security Services;
* information security in the agency, for reducing risk exposure, and for ensuring the agency’s activities do not introduce undue risk to the enterprise;
* ensuring compliance with state enterprise security policies, standards, and security initiatives, and with state and federal law and regulations.

**Cyber Security Services (CSS)**

CSS will be responsible for managing all response efforts in accordance with the [Statewide Information Security Incident Response Plan](https://www.oregon.gov/das/OSCIO/Documents/InformationSecurityIncidentResponsePlan.pdf).

# Approval

Name, title Date

Name, title Date

# Appendix A: Agency Data Breach Reporting Protocol

(Actions during an actual or suspected data breach)

**This includes executive department boards, officers, commissions, departments, divisions, and other entities subject to the State CIO’s authority for information systems security under ORS 276A.300**

**Step One—Notify CSS**: If an incident or breach has occurred or is occurring, contact the Cyber Security Services (CSS) Hotline at 503-378-5930 promptly, but no later than 24 hours from the time the incident or breach is discovered. Provide specific point(s) of contact to CSS for coordination and all information available at the time of notification.

**Step Two—CSS Assessment**: CSS will direct the review and categorization of the incident, and oversee the development of the incident response plan. Note any overlap with Step Three. CSS will:

1. Notify the State CIO and Agency Senior Portfolio Manager.
2. Contact the Department of Justice, Business Transaction Section, for advice about the incident, including on criteria for the breach of personal or other regulated information.
3. Assist agency leadership with answering key questions, such as:
   1. What type of data was potentially compromised?
   2. How many individuals may have been impacted?
   3. How, where, and when did the potential compromise occur?
   4. What is the plan to determine if information was compromised?
   5. Was there a contractor or employee involved who violated the law or state policy?
4. Direct development of the incident response plan, including timelines, communications, and required parties, and designation of an incident commander.

**Step Three—State Notifications**: Some information may not be available within the timeline required below, and may change over the course of the investigation. The agency and CSS will agree to a schedule for providing regular updates as part of developing the incident response plan (Step Two). At least the following offices and agencies must be notified:

1. Within 48 hours of incident discovery, the agency will notify the Governor’s office policy advisor about the incident, and provide available answers to the questions above.
2. Within 48 hours of the time an incident with criminal implications has been verified, the agency will contact the duty supervisor at the Northern Command Center of the Oregon State Police at 503-375-3555.
3. Within 24 hours of verification of any loss or compromise of Criminal Justice Information, CSS will contact the Oregon State Police Information Security Officer.
4. The agency will report the incident to the Legislative Fiscal Office, in accordance with ORS 276A.306.
5. The agency will notify its human resource department if the incident is the result of an employee violating agency policy.

**Step Four—Media and Community Partner Notification**: In accordance with the CSS-approved incident response plan, media release will be sent from the agency. CSS communications will assist the agency with media release preparation. The Agency will inform its staff of the incident or breach, and then send the initial media release. The agency and CSS will agree to a schedule for providing regular updates as part of developing the incident response plan (Step Two).

**Step Five—Regulatory Notifications**: The Agency may need to notify regulatory agencies if regulated data was involved. In accordance with the CSS-approved incident response plan, the agency will work with the State CIO, CSS, DOJ counsel, Legislative Fiscal Office, Governor’s office, and its own internal communications office to determine appropriate actions and timelines as part of developing the incident response plan (Step Two).