State of Oregon

Information Security Incident Response Plan

ENTERPRISE
information services

TABLE OF CONTENTS

INTRODUCTION

Information security incidents affect the state's enterprise information assets and its ability to provide services to citizens of Oregon. Incidents must be investigated and a response prepared to mitigate the state's risk. Because of inter-related data processing and public perception of the State as a single entity, information security incidents at individual agencies may impact other state agencies or the State as a whole. Incident response activities must be effective, coordinated, and protect the interests of individual agencies, the state as a whole, and of the citizens they serve.

Cyber Security Services has developed this Incident Response Plan to guide response to information security incidents. This plan is built on the premises that incidents vary in severity and require a flexible scale of response efforts to mitigate, and that response efforts must be adequate, uniform and coordinated regardless of the size. Small, single agency incidents may only require the directed efforts of a small agency team to mitigate, while large, multi-agency incidents may require close coordination between agencies under centralized direction from the DAS Director, the State CIO, or the Governor's Office. This plan presents a response, communications and escalation structure flexible enough to address incidents of any size or scope.

This document describes how resources are to be brought together to respond to an information security incident. The objectives of the incident response plan are to facilitate quick and efficient response to incidents, limiting their impact and protecting State information assets. The incident response plan defines roles and responsibilities, documents the steps necessary for effectively managing an information security incident, describes incident severity levels and how escalation occurs, pre-defines communications channels and prescribes necessary education to achieve these objectives.

AUTHORITY

ORS 276A.300 directs the Office of the State Chief Information Officer to develop and implement policies for responding to incidents that involve information security. The State CISO has the ultimate authority to determine when an incident has occurred, and is directed to take any required steps necessary to respond to incidents to prevent or mitigate damage caused by an incident.

Statewide information security policies:

Policy Number	Policy Title	Effective Date
107-004-050	Information Asset Classification	1/31/2008
107-004-051	Controlling Portable and Removable Storage Devices	7/30/2007
107-004-052	Information Security	11/16/2020
107-004-053	Employee Security	7/30/2007
107-004-100	Transporting Information Assets	1/31/2008
107-004-120	Information Security Incident Response	11/16/2020
107-104-140	Privileged Access to Information Systems	7/10/2013
107-104-150	Cloud and Hosted Systems Policy	5/1/2019

TERMS AND DEFINITIONS

Asset. Anything that has value to the agency.

Control. Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, physical, management, or legal nature.

Incident. A single or a series of unwanted or unexpected information security events (see definition of "information security event") that result in harm, or pose a significant threat of harm to information assets and require non-routine preventative or corrective action.

Incident Command System (ICS). A standardized incident management approach that allows for the integration of facilities, equipment, personnel, procedures and communications within a common organizational structure; enables a coordinated response among different agencies and entities; and establishes common processes for planning and managing resources.

Incident Commander. The Incident Commander has overall responsibility for managing the incident by establishing objectives, planning strategies, and implementing tactics. The Incident Commander is the only position that is always staffed in an Incident Command System (ICS) application. On small incidents and events, one person, the Incident Commander, may accomplish all management functions. The Incident Commander is responsible for all ICS management functions until he or she delegates those functions.

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) of the series of steps taken when responding to incidents.

Incident Response Program. Combination of incident response policy, plan, and procedures.

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
- E-mails or messaging system conversations and their attachments
- Audio and video files
- Images, graphics, pictures and photographs
- Programs, software, and macros

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.

Information Security Event. An observable, measurable occurrence in respect to an information asset that is a deviation from normal operations.

Incident Response Team (IRT). Team of responders, composed of both CSS SOC and Agency personnel, to an information security incident. Although the makeup of the team may vary depending upon incident scope and severity, it will contain the following common elements regardless of size: an incident command structure, a communications component and information security technical advisors.

ROLES AND RESPONSIBILITIES

State Chief Information Officer (CIO). Leads state government in enterprise information technology management, strategic planning and policy. The CIO may step in as Incident Commander for incidents Level 2, 3, or 4 depending on scope of incident.

State Chief Information Security Officer (CISO). Responsible for statewide information security.

Cyber Security Services (CSS). The CSS manages the state's response to incidents including those involving an actual or suspected breach under the Oregon Consumer Identity Theft 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.

Office of Emergency Management (OEM). Responsible for maintaining the state Emergency Operations Plan and managing the Emergency Coordination Center (ECC) facility. Maintains a state-wide common operating picture and coordinates emergency response and recovery activities across local, tribal, state, and federal governments and the private sector. In incidents classified as Levels 3 or 4, may be called upon to facilitate coordination of response efforts.

State Agency Director. Accountable for safeguarding agency information and information systems. In Level 1 incidents where the agency has requested CSS assistance, CSS will provide response and advisory capabilities as requested when possible. In incidents classified as Levels 2, 3 or 4, a Unified Command structure may be utilized in which agency directors will coordinate actions and communications with the CSS and will assist the SIRT in response activities. Agency directors are also responsible for representing the agency business owner and for providing business continuity response and leadership in the event a security incident jeopardizes the on-going business operation of the agency.

Agency Incident Response Point of Contact. Responsible for establishing agency reporting method and communicating incidents with CSS SOC. Provides a point of contact for communications between CSS SOC and agency responders during an incident.

Legal Counsel. Responsible for providing legal guidance in all stages of incident response activities.

Public Information Office. Responsible for coordinated release of information about incidents to the public, under the direction of the Incident Commander. In the event of a public release and depending upon the scope of the incident, agency Public Information Offices will work together with EIS's and the Governor's Office's PIOs to provide a unified message to the public.

PROGRAM

The Statewide Incident Response Program is composed of this plan in conjunction with the Statewide Information Security Incident Response Policy number 107-004-120 and procedures.

Rules of Engagement

Agencies will report information security incidents to the CSS within the timeframe specified by the statewide Incident Response policy. Upon being contacted, the CSS will assign an incident coordinator and assess the severity and impact of the incident. The CSS may bring in additional resources and form an expanded IRT, depending upon incident severity, size and scope. If needed or requested, the CSS SOC may perform various roles in responding to the incident, including incident command, physical response, forensic analysis, or other roles as needed.

When responding to an incident with an agency, the following are rules of engagement between the CSS SOC and agencies:

- Mutual respect of authority and business requirements.
- Agencies will advise the CSS SOC of potential incidents in a timely manner.
- The CSS SOC, in conjunction with agency director and business owner, may request or require problem hosts or networks be disconnected from the statewide network and/or the Internet if needed for containment.
- Agency computer resources may be quarantined for forensic investigation.
- Agency director and business owner will actively participate in all discussion that would affect agency business.
- Agencies will provide resources to assist the CSS SOC to expedite investigations, containment, and resolution of an incident.
- The CSS SOC, potentially including Legal Counsel and Public Information Officer, will work with agencies to determine if, when and how external resources will be notified.
- The CSS SOC will coordinate with agency incident commander(s) responsible for leading business continuity efforts that may result from an incident.
- Agencies and the CSS SOC will maintain clear communications between incident responders.
- Agencies and the CSS SOC will work in accordance with state and agency policies.
- The CSS SOC may require agencies to implement mitigating actions (e.g. patches, firewall rules) in a timely manner.
- Agencies and the CSS SOC will work together on post-incident activities such as remediation and lessons learned.

Because of the sensitivity of incident information and the high potential for damage caused by inappropriate release of it, all parties involved in responding to an incident will adhere to the following practices regarding agency information:

- Default classification level for all communications within the IRT will be level 3 (as defined in the statewide Information Asset Classification policy 107-004-050). IRT members will reinforce this message as appropriate with other participants during an incident.
- Information not to be shared outside incident meetings must be identified by agency personnel and will not be included in minutes or any other media that might become public record or be otherwise released.
- Potentially public information brought to the IRT will not be shared without specific discussion with the agency, Legal Counsel and Public Information Officer prior to authorization and release.
- Information about an incident will not be released to any unauthorized party.
- When it is deemed by the CSS SOC that technical details of an incident will benefit other state agencies or the public as a whole, redacted details of the incident will be shared as it is deemed appropriate and confidentiality can be preserved.

Exercises

To test the incident response plan and verify the CSS SOC's ability to execute, information security incident exercise will be planned and conducted as necessary, depending upon the level of recent CSS SOC activity. Specifically, these exercises will:

- Test the team response using the plan.
- Identify updates to the plan as necessary.
- Verify contact numbers and test communications and escalation.

The CSS SOC will encourage and assist agencies to exercise their own incident response exercises, including interactions with the CSS SOC.

Incident Response Command

NIMS describes three types of incident command structures:

- An Incident Commander is in charge of directing all incident response activities. This structure works best for incidents that occur under one jurisdictional authority.
- A Unified Command structure, where individuals designated by their organizational authorities work together to respond to the incident. This structure works best for larger incidents that span multiple jurisdictions.
- An Area Command structure, where an organization provides oversight to disparate incident response groups responding to a complex incident. This structure is typically activated if necessary for non-site specific, large scale or long-term incidents.

In an environment such as Oregon state government, where agencies are accountable for the security of their individual IT resources, but CSS is responsible enterprise security, including incident response, the structure of incident command may vary on an incident-by-incident basis or in response to changing conditions. Agency and CSS SOC incident response must be flexible and allow transition between different incident command structures as part of the escalation process.

Incident Response Team

The size and makeup of the incident response team will be determined by the nature, scope and severity of the incident. Small, Level 1 incidents may require only a few agency staff and minimal or no participation by the CSS SOC. Larger incidents, especially ones with multi-agency impact, may require a response team consisting of CSS SOC and agency staff working together. The largest incidents may require extensive use of third-party, contracted response resources.

Because response team makeup and size can vary widely, the state must be able to flexibly and quickly increase team size and capability to meet the needs of potentially large incidents. In order to maintain team flexibility and to promote incident response expertise in the state, the CSS will identify, train and maintain a staff of security experts drawn from the SOC. Similar to a group of volunteer fire fighters, in an incident emergency the State CISO may call on experts from state agencies to assist with response efforts. During response activities these volunteers will be under the direction of the State CISO for all incident-related activity.

Although the bulk of these volunteers will be information security and technical subject matter experts, there are other areas of expertise that are routinely required for incident response. Examples include Public Information Officers (PIOs) and attorneys. The CSS SOC will identify professionals in these areas, provide training in security incident response as it relates to their fields, and incorporate them into the IRT as necessary to provide specialized expertise to the team during an incident.

In the event of a very large-scale incident, the internal resources available to the CSS SOC may be insufficient. The CSS will establish and maintain contractual resources that can be used to hire third-party expertise and capacity to assist with incident response activities as needed. Those resources will include vendors capable of large-scale incident response.

Response Processes

CSS SOC response activities generally follow the incident response handling stages as described in NIST Special Publication 800-61. Although detailed description of these steps is outside the scope of this plan, and instead are detailed in the Incident Response Procedures, a brief overview is provided here of the incident handling stages:

Preparation

In general, the CSS's preparation responsibilities include not only its own preparedness but also assisting agencies in their preparation efforts. Other sections of this document (Exercises, Education and Awareness, Communications) describe one aspect of the CSS's response preparedness activities.

Identification

Identification involves the processes of incident detection and alerting; initial fact finding; and, the determination of Agency capabilities. These activities and the information derived from them help CSS determine how many resources to engage and what level of support to provide going into the next stage.

Scoping and Classification

Properly scoping an incident is likely the single most important part of incident response—without knowing how wide and deep your problem goes, it'd be next to impossible to respond and resolve it effectively and efficiently the first time. Scoping will involve initial and follow-up triage, and preliminary forensics.

Performing a proper scoping exercise, and then performing business impact analysis as well as, potentially, correlating to past or on-going incidents will provide the necessary information to classify the incident. Classification levels inform the level of involvement of CSS resources and the command structure.

After Classification, start defining the communications parameters, such as who to notify and when; who's commanding the incident; and what methods are acceptable for different communications types. Communications need to be properly managed throughout the entirety of the incident.

Containment

Incident containment is critical in the enterprise environment and is a primary concern of the IRT. Failure to adequately contain an incident increases the scope and impact and is a common trigger for escalation of incident severity. Develop a comprehensive and thought-out containment plan; do not piece meal ad hoc containment efforts.

Containment must include not only reacting to the incident cause itself but also limiting communication about an incident to only those with a need to know. Loss of communications control can easily result in adverse publicity and increases the difficulty of managing an incident.

Eradication and Recovery

After an incident has been contained, it is critical to confirm all threats and vulnerabilities have been successfully mitigated and that new threats or vulnerabilities have not been introduced. The CSS SOC will assist agencies through the process of verifying eradication was successful and related information is intact and secure before impacted services are restored.

Agency business and IT processes will largely drive incident recovery. The CSS SOC may provide information security guidance during the recovery process.

Post-Incident Activity

Post-incident activities that the CSS may perform include lessons-learned activities with affected agencies, sharing sanitized incident information with other agencies or external entities for knowledge dissemination, recommending or performing vulnerability assessments or other information security practices, and altering enterprise incident response processes to reflect lessons learned during the incident.

Incident Severity and Classification

Incident severity determination answers the question "**what is the overall impact of the incident on the State of Oregon?**" Accordingly, incident severity ratings drive incident routing, escalation, escalation urgency, and composition of the IRT to respond appropriately to incidents. Incident severity may change during the course of response activities in response to factors such as scope change, increased publicity or other escalation factor.

The following factors are example considerations when classifying the severity of incidents:

- Criticality of systems that are (or could be) impacted
- Value and sensitivity of the information compromised (if any)
- Number of people or functions impacted
- Political sensitivity
- Press involvement or publicity
- Enterprise impact, including reputational and legal harm
- Multi-agency scope

The CSS SOC uses the following incident classification levels:

Level 0 – Event Triage.
Upon initial detection of an anomalous event, the agency must determine whether the event is an incident that requires non-routine incident response activities.

Level 1 - Minor:
Incidents of minor impact that are resolved with minimal disruption of normal activities—there is no need for creation of an expanded IRT. Incidents with Level 1 impact are the most common. Incident handling activities will be performed by the state agency with minimal assistance from CSS or other state resources. Examples include: miss-mailing of a limited number of sensitive documents, theft of a laptop with little or no sensitive information, and malware infection requiring non-routine mitigation activity.

There is little or no likelihood of press involvement and no potential for statewide impact. This is the default, minimum, classification for incidents reported by agencies.

Level 2 - Medium:
Incidents having “hard cost” impacts and requiring nontrivial and coordinated response activity that is not part of normal operations may require the creation of an expanded IRT. The specific resources required for the expanded IRT will vary depending on the incident characteristics. Examples of Level 2 incidents include malware outbreaks that impact multiple workstations and/or servers, persistent hacking activity that requires coordinated CSS/agency response, etc. Level 2 incidents may have significant impact to one agency, may require escalation to the CSS SOC for response, and may have the potential for media coverage. Typically, IRTs response to Level 2 incidents could include any/all of the following:

- Information Security & Technology Subject Matter Experts
    - ▫ Network Administrators
    - ▫ Server Administrators
    - ▫ Desktop Administrators
    - ▫ Application Developers (Dev) and QA
- Computer Forensics
- Legal Counsel
- Agency Privacy Office Representatives (in cases of Privacy Incidents)
- Agency Business Representatives
- Agency Public Information Office

Level 3 - Major:
Level 3 incidents have major business impact (e.g. incidents involving civil penalties, major privacy breach notification activities, prolonged business disruption, loss of critical services to Oregon residents, etc.) and always require the formation of an expanded IRT, including possible mobilization of 3rd-party retainers.

They may be multi-agency with wide spread impact and have statewide press coverage. They may have political impact to State government. Examples of Level 3 incidents include: successful coordinated hacking activity, publicized extortion attempts by hackers, Denial-of-Service (DoS) attacks against significant infrastructure, a database breach and potential release of PII, or a malware outbreak spreading across multiple agencies.

IRT response to Level 3 incidents could include any/all of the following:

- Incident Command will happen at a top agency or multi-agency level
- Information Security, Incident Response & Technology Subject Matter Experts from agencies and the DCS
- Agency Privacy Office Representatives (in cases of Security/Privacy Incidents)
- Agency Business Representatives
- Legal Counsel
- If criminal, the Oregon State Police (OSP) or other law enforcement

In addition, Level 3 (and Level 4) incidents should follow the communications guidelines in the Executive Branch Agency Breach Response Protocol regardless if there is a detected data breach.

Level 4 - Critical:
Level 4 incidents have the highest level of impact to state systems or government and always require the formation of an expanded IRT commanded at a high level. They may have scope beyond just state agencies (public/private) or be multi-state, may have high impact to citizens, and national press interest. Political impact from the incident could be major. Examples of Level 4 incidents include: Denial-of-Service (DoS) attacks against major infrastructure, terrorist activity, multi-state or national level incidents.

IRT response to Level 4 incidents could involve any/all of the following:

- Incident Command directed from the highest level: Governor, or State CIO
- Information Security & Technology Subject Matter Experts
- Coordination by multiple Agency Directors and agencies
- Coordination with national law enforcement
- Department of Justice (DOJ)
- Office of Emergency Management (OEM)
- Coordinated, strategic Press Communications
- Business Continuity Representatives
- External Subject Matter Experts (e.g. incident response experts)
- Legal Counsel

The CSS SOC will classify incidents reported to them according to the criteria above and respond to them accordingly. The CSS SOC may reclassify and escalate incidents as conditions change and may require agencies to take action based upon the enterprise incident classification.

Escalation

Different level incidents require different types of resources, communication strategies and levels of authority to respond. Incidents and response circumstances may change, often quickly, requiring smooth escalation of response efforts.

Escalation is generally triggered by the following types of events:

- **Publicity:** Public or Press interest in an incident may increase the sensitivity, urgency and resource requirements
- **Scope Change:** The scope of the incident may increase
- **Responsibility or Authority Change:** Responsibility or Authority to respond may be transferred
- **Resource Constraints:** The capacity or capabilities of current responders may be exceeded
- **Political sensitivity:** Potential political damage may require a higher-level response
- **Perceived or actual mismanagement:** Initial response may be (deemed) inadequate, requiring a higher-level response

An escalation requires transfer of authority and incident command to a responder appropriate for the new level of response, including possible transition to a new incident command structure. Additionally, it may require opening communications with other parties, bringing new resources online and coordination with current response activities and personnel.

Incident

ESCALATION AND ESCALATION-BASED COMMUNICATIONS

ESCALATION TRIGGERS

- Publicity
- Scope
- Responsibility/authority
- Lack of resources
- Political sensitivity
- Mismanagement (perceived or actual)

Escalation Level	Involved Parties	Communications*
LEVEL 0 **Example Triggers:** Initial detection, routine, triage	Agency IT Staff	**Agency Notifies** • Internal Staff (as applicable)
LEVEL 1 **Example Triggers:** Agency determines that it meets definition of Incident	• Agency IT Staff • CSS SOC (advisory as applicable) • DCS Staff (as applicable) • No/Little Management Involvement	**Agency Notifies** • CSS
LEVEL 2 **Example Triggers:** • Significant impact to 1 agency • Potential or actual media coverage	• Agency CIO • Agency PIO • CSS SOC • State CISO • Agency Management (as applicable)	**Agency/CSS Notifies** • DOJ (as applicable) **CSS Notifies** • State CISO • LFO
LEVEL 3 **Example Triggers:** • Multi-Agency, wide spread impact • Significant impact to multiple agencies Statewide press coverage • Potential for serious impact to state (e.g. reputation, regulatory)	• Agency Executive Management (as applicable) • Agency CISO/CIO(s) (multiple agencies) • Agency/State/Governor’s PIO • CSS SOC • State CISO • State CIO • DCS Administrator (as applicable) • DOJ	**CSS Notifies** • Governor’s Office • State CIO (if not already involved) • (Optional) OEM/OERS at 1.800.452.0311 **CSS/Agency consider** • Law enforcement (consult DOJ)
LEVEL 4 **Example Triggers:** • Scope beyond just State Agencies (public/private) • High impact to citizens • National press interest • Serious statewide or multi-state impact	**ECC ACTIVATED** • Governor Representative • State CISO • State CIO (as applicable) • DCS Administrator (as applicable) • Agency Director (as applicable) • Agency/State/Governor’s PIO (as applicable) • DAS Director • TAG – OEM • Governor RPC (as applicable) EO 08-20 • Governor GRC (as applicable) EO 08-20 • DOJ	**CSS Notifies** (if not already involved) • MS-ISAC • Fusion Center • OEM/OERS *Communications should be assumed to be additive, whereby lower levels also includes the notifications of the previous level(s).

COMMUNICATIONS

Maintaining communications security is critical while responding to information security incidents for the following reasons:

- **Adversarial conditions:** information security incidents are frequently the result of malicious attack. Responders must avoid disclosing information about response efforts that might help attackers. Careful analysis of potential information leakage channels and tight control of information disclosure can be critical. For example, if an attacker has compromised credentials to an email system, relying on that system to communicate about the incident may share information that will help the attacker. Attackers may also monitor public information channels so care must be taken not to disclose information that could help them understand effectiveness of their tactics or state defenses.
- **Reputational harm:** a primary goal of incident response is to minimize the impact of an incident. Damage to the state's reputation can represent a huge impact if an incident undermines the public's confidence in State information systems and personnel. Messaging to the public is a critical component of incident response activities.
- **Information sensitivity:** the subject information involved in an investigation may be sensitive and must be protected appropriately. The incident investigation must not endanger the information it's protecting.

Need-to-Know

Every effort must be taken to preserve the confidentiality of incidents; for that reason, all communications shall be on a need to know basis. At no time should incident response information be shared unless the recipient has a valid need for it, and careful consideration should be given to appropriate messaging for specific audiences.

Incident Response Team Internal Communications – Because of the sensitive and confidential nature of information and communication surrounding an incident, all communication must be conducted through channels appropriate to the security needs of the information. In general, the CSS considers telephones sufficiently secure for use during incidents and is a generally acceptable method of response team communications. Explicit consideration should be given to the security of electronic communications methods, such as email, to determine whether they are adequately secure for a specific incident. Because of their integration with email, voicemail and faxes should also be used with caution for sensitive information. Information classified as Level 3 or Level 4 must be protected at all times in accordance with the Enterprise Information Security Standards (i.e. encrypted in transit).

Incident Communication

After being notified of an incident, the CSS will determine scope and severity, and then activate members of the IRT as necessary. Scope, severity and IRT team membership also determines the participation in incident communications.

Communication Management Plan Requirements

Following are the major components of incident communications within the IRT:

- A comprehensive list of key contacts that need to be regularly updated with status information.
- Contact details for all parties requiring updates.
- The different types of updates that will be required. Different update messages may be required, depending on the level of the incident and the audience receiving the communication:
    - In order to facilitate escalation, potential responders should be prepped before being activated at their severity level.
    - Senior management update (State Chief Information Officer, State Chief Information Security Officer, and State Chief Operations Officer)
    - Legal Counsel should be consulted before any public information release or any consultation with law enforcement
    - Public Information Officer should be prepped and involved in any incident that may involve press communications
    - Agency Chief Information Officer (CIO)
    - Agency Director and Business Owner
- How often each type of update is required and when the next one is due.

Third-Party Notifications

Third party notifications may take place in accordance with the following general guidelines:

- To fulfill legal or contractual obligations
- Incident details may be shared with a third party if doing so may help them prevent their own incident
- Involve third parties when they may be able to help incident response, taking care to balance any cost of that help against potential benefits

Press communications external to the IRT will be handled by the agency PIOs or the Governor's PIO, in combination with EIS PIOs, as appropriate. Legal council should be consulted before any major press communication. Major components may include:

- Who is authorized to release each different update statement?
- The mechanism by which each update will be communicated.
- A process for vetting information to be disclosed and agreeing upon content
- The different types of updates that will be required. Different update messages may be required, depending on the audience receiving the communication:
    - Impacted agency staff
    - Other State of Oregon staff
    - Update for customers and business partners
    - Press/media statement where required
    - Public communication (e.g., social media regarding the status of incident response, written notification following a breach, etc.) where required
    - Update for emergency services/authorities

Audience/Recipients

Potential recipients of information from IRT activities may include:

- **Office of the Governor:** CSS SOC will communicate with the Office of the Governor to keep the governor informed of any activity that may escalate or may result in a major media event.
- **State Chief Information Security Officer:** The State Chief Information Security Officer and designated members of the CSS will receive any information they request concerning an information security incident or related matter referred to them for resolution.
- **IRT members:** Members of the IRT are also, by virtue of their responsibilities, trusted with confidential information. Others involved in resolving a security incident will be given only the confidential information they must have or they require to secure their own systems.
- **Other Agencies and Response Teams:** Other agencies will be trusted with incident information to allow them to effectively respond. Information may be shared with agencies not directly involved with incident response activities if doing so will help protect those parties. In this case, information will be limited to what is helpful to prevent further outbreaks or future incidents.
- **Oregon Emergency Management:** SIRT will coordinate with Oregon Emergency Management to facilitate coordinated State and local government communications during incidents, as appropriate.
- **Other State, Local or Federal government agencies and entities:** Potential contacts include: US Computer Emergency Readiness Team (USCERT), the state Fusion Center, the state enterprise Business Continuity Team, law enforcement, Homeland Security and the Multi-State Information Sharing Analysis Center (MS-ISAC). The CSS SOC may share information with these entities to assist in broader incident response efforts but always within the constraints of protecting agency and state interests
- **Public at Large:** The public at large will receive no restricted information. Communication with the public will be closely controlled and monitored by agency, DAS PIOs, or the JIC, as appropriate, and under the advice of Legal Counsel. It is important that PIOs and the JIC recognize that the information made available to State of Oregon employees is in effect made available to the community at large, and will tailor the information accordingly.
- **Media:** The media also are considered part of the general public. PIOs will manage communications to the media, with the assistance of the CSS SOC.
- **State of Oregon employees:** Users of computer systems owned and/or operated by the State of Oregon are entitled to information that pertains to the security of their own computer accounts. Users are entitled to be notified if their account is believed to have been compromised or they may suffer personal loss.

The general State of Oregon user community will receive no restricted information, except where the affected parties have given permission for the information to be disseminated. Statistical information may be made available to the general user community. There is no obligation on the part of the CSS SOC to report incidents to the community, though it may choose to do so. CSS SOC may decide to inform all affected parties of the ways in which they were impacted, as well as mitigating actions they should take, or to encourage the affected agency(s) to do so.

- **External Information Security Resources:** The information security community will be treated as general public. While members of IRT may participate in discussions within the information security community, such as mailing lists, blogs and conferences, they will treat such forums as though they were the public at large.

  While technical issues (including vulnerabilities) may be discussed to any level of detail, any examples from IRT experiences will be anonymized to avoid identifying the affected parties.

- **Law Enforcement:** IRT will cooperate fully with law enforcement to provide information that is legally required. IRT may consult with or request law enforcement assistance in an incident investigation.
- **State of Oregon Management:** Because of the nature of their responsibilities and consequent expectations of confidentiality, members of State of Oregon management are entitled to receive information necessary to facilitate the handling of information security incidents that occur in areas for which they have management responsibilities.
- **Vendors or manufacturers of involved hardware or software or service providers:** The CSS encourages vendors of networking and computer equipment, software, and services to improve the security of their products. To support this, a vulnerability discovered in such a product will be reported to its vendor, along with all technical details needed to verify the problem. Identifying details will not be given to the vendor without the permission of the affected parties.

  Vendors, manufacturers or service providers may be a valuable resource to the IRT for incident response. In this situation, only the information necessary to enable them to provide the desired assistance will be shared. If confidential or sensitive information must be shared, appropriate contractual documents will be executed.

EXPERTISE, EDUCATION AND AWARENESS

The Cyber Security Services (CSS) Security Training and Awareness Program is a continuous effort to educate and empower the state's workforce to adopt good security habits at work, at home and while mobile. The goal of the awareness program is to reduce human vulnerabilities that could result in a breach of confidentiality, integrity, and availability of state information assets, thereby increasing the overall security posture of the state.

The focus of the CSS awareness program is to change human behavior that increases information risk by implementing a robust awareness program. The awareness program targets the State's workforce, including employees, contractors, and volunteers, through a variety of training materials, services, and delivery platforms.

Cyber Security Services

The CSS team members are required to maintain professional and subject matter expertise in all aspects of information security, incident response and forensics. The team will identify and attend appropriate training and maintain appropriate certifications.

Agency incident responder training

Agencies are responsible for exercising their incident response plans. CSS recommends that agencies with nascent, or without, experience exercising their plans coordinate their first exercise with CSS or a reputable vendor. Agencies are also responsible for maintaining the technical and business expertise to operate and maintain their information systems.

COMPLIANCE

All agencies are subject to the Oregon Consumer Information Protection Act (OCIPA) (ORS 646A-600). Although OCIPA details one type of data breach, it is the responsibility and purview of CSS to declare data breaches in all cases. The CSS recognizes agencies may be subject to additional regulations, which must be addressed in each agency's incident response plan, and will support agencies in their effort.

IMPLEMENTATION

The CSS is committed to assist agencies in formulating and implementing appropriate response strategies. This plan was developed to achieve this goal by giving direction and support for the statewide Information Security Incident Response policy.

CSS will:

- Respond to state information security incidents.
- Serve as core staff within the Incident Command Structure for incidents classified as Level 2, 3 or 4.
- Maintain trained technical staff with the capability to forensically gather and analyze evidence while observing necessary evidence-preservation practices.
- Maintain a computer forensics lab and perform forensic services for agencies as part of the incident response process.
- Test the incident response plan and verify CSS SOC's ability to execute.
- Maintain a comprehensive list of key contacts that is regularly updated with status information.
- Provide or recommend basic incident response training covering incident identification and an overview of an incident response plan.
- Make recommendations for specific training or courses.
- Provide education or guidelines on the accurate and timely identification and escalation of incidents.

APPROVAL

By: ______________________________ 04/05/2021

Terrence Woods, State Chief Information Officer Date

By: Gary A. Johnson ______________________________ 04/05/2021

Gary Johnson, State Chief Information Security Officer Date

APPENDIX A - DATA BREACH REPORTING PROTOCOL

Executive Branch Agency Breach Response Protocol

(Actions during an actual or suspected 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 security 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 the timelines required under Step Three. CSS will:

1) Notify the State CIO or Deputy State CIO.
2) Contact the Department of Justice, Business Transactions 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:
   - What type of data was potentially compromised?
   - How many individuals may have been impacted?
   - How, where, and when did the potential compromise occur?
   - What is the plan to determine if information was compromised?
   - 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 a 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 and the State CISO or his designee will jointly 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) CSS 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 and other DAS communications staff will assist with media release preparation. The State CISO or Deputy State CISO or their designee will review and approve any media communications prior to release. 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 internal communications office to determine appropriate actions and timelines as part of developing the incident response plan (Step Two)

ENTERPRISE
information services