# PURPOSE

To ensure the scope and impact of IT security incidents are properly evaluated, and that a coordinated, centralized approach is used to determine if, when and how to communicate notification of an incident.

# POLICY STATEMENT

The state recognizes its duty and obligation to disclose any breach of a security system that results in the unauthorized disclosure of personal information pursuant to RCW 42.56.590 *Personal information — Notice of security breaches*. In accordance with this Section, the timing of the disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

It is also recognized that:

- Not all IT security incidents result in a breach or level of severity that requires notification of disclosure.
- Until a vulnerability or threat can be properly identified, contained and mitigated, it should be assumed that a vulnerability exploited in one agency could be leveraged to pose threats to multiple agencies.
- Unnecessary or ill-timed disclosure of incidents could provide adversarial parties with information that could be used to degrade the confidentiality, integrity and availability of state systems and data such that citizens' personal data could be vulnerable.

The purpose of this policy is to ensure that:

1. The scope and impact of state government IT security incidents are properly evaluated and mitigated, and that communication regarding incidents is contained so that vulnerabilities are not exposed to adversarial parties.
2. A coordinated, centralized approach is used to determine how and when to communicate notification of an incident within the state and when required by state law.

# Response Process

Response to an IT Security Incident, once discovered, shall be governed by the following process. For each step, with the exception of Step 5, the degree to which information regarding an incident can be shared, and with whom, shall be in accordance with Traffic Light Protocol (TLP) RED. This means that recipients of IT Security Incident information may not share information with any parties outside the specific exchange, meeting or conversation in which it was originally disclosed. The Traffic Light Protocol is a set of designations, developed by the United States Computer Emergency Readiness Team (US-CERT), that are used to ensure that sensitive information is shared with the appropriate audience. Information on the TLP designations, including when they should be used and how information may be shared, is found in Attachment 1 to this Policy.

Step 1. Agencies shall report all IT security incidents to the State Chief Information Security Officer (CISO).

- Regardless of the perceived scope or impact of an IT Security Incident, as soon as possible, but not later than 48 hours after discovery of an incident, the agency Chief Information Officer (CIO), Chief Security Officer or person otherwise responsible for agency IT security shall immediately notify the State Chief Information Security Officer (CISO) and the Security Operations Center (SOC) at Consolidated Technology Services (CTS). Incidents to be reported apply to systems and data operated and maintained by the agency within the state network or to any external system managed or maintained by a third-party (e.g. cloud service provider).
- If the agency was made aware of the incident by persons external to the agency, or external parties are already involved, the agency shall provide contact information for these persons to the CISO and/or SOC at CTS.
- Shared e-mail services shall not be used to notify the CISO and/or SOC of the incident. Notification shall be provided by phone or other secure electronic means.

**Step 2. State CISO and CTS SOC shall investigate to determine degree of severity and assist with mitigation.**

- **Upon being notified by an agency, the CISO and/or his/her staff will promptly work with agency IT security staff and any identified external parties to determine the scope and severity of the incident. The CISO will provide assistance to the agency to identify the cause of the incident and determine what corrective steps should be taken to eliminate any identified vulnerabilities.**
- **In addition, the CISO shall:**
  - **Determine whether the impacts of the incident are confined to the single agency or may affect multiple agencies.**
  - **Work with law enforcement agencies if necessary to gather additional information and assists with their investigations.**
  - **Provide available tools to the agency to help analyze the current incident and prevent future occurrences.**

**Step 3. State CISO shall notify the state CIO. (if required)**

- **After analysis of the incident, the CISO, at his/her discretion, will notify the state CIO and the Assistant Attorney General for the Office of the Chief Information Officer (OCIO) to provide details on the nature, scope and possible impacts of the incident and provide recommendations on what, if any, further actions should be taken.**
- **Notification to the state CIO will include:**
  - **Type and magnitude of the incident**
  - **Whether one, or more than one, agency was impacted**
  - **Steps taken to identify the source and impact of the incident**
  - **Whether the incident has been successfully mitigated**
  - **What steps remain to be taken to mitigate risk**
  - **Estimated timeline to complete mitigation in order to eliminate additional risk or exposure to the state.**
- **At this time the CISO, in conjunction with the Washington State Office of the Attorney General, will also provide the state CIO with an informed opinion as to whether or not the severity of the incident's impact warrants public notification as required by law.**

**Step 4. State CIO will convene Security Incident Communication Team (SICT). (if required)**

- **Should it be determined by the CIO that public notification of an IT Security Incident is required by law, the CIO, at his/her discretion, will promptly convene a Security Incident Communication Team. The composition of the SICT will be at the discretion of the CIO, but may include:**
  - **Heads of the agency or agencies impacted**
  - **Director of CTS**
  - **Impacted agency(s) CIO**
  - **State CISO**
  - **Legal Counsel**
  - **Members of law enforcement**
- **The state CIO will notify the Governor's office that an incident has occurred and may require public disclosure.**
- **In preparation for notification of an IT Security Incident as required by Chapter 42.56.590 RCW, the SICT will, in the most expedient manner possible:**
  - **Identify appropriate legal, financial or other non-technical remediation measures in the event they are necessary.**
  - **Develop a cohesive, comprehensive communication plan that accurately describes the nature of the incident and impact it may have on affected parties.**

**Step 5. State CIO will authorize and coordinate release of public notification with breached agency(s) (if required)**

- **Agencies will fully cooperate with the Governor's office in support of disclosure of the incident, and will coordinate with the CIO on any requests from the public for information related to the incident.**
- **TLP Designation: WHITE.**

# DEFINITIONS

**IT Security Incident: Any unplanned or suspected event that could pose a threat to the integrity, availability or confidentiality of an Agency's, or the State's, data or systems.**

# RESPONSIBILITIES

**State Chief Information Officer (or designee)**

- Interpret the policy.
- Update this policy and related resources as needed.

### Technology Services Board (TSB)

- Review and approve major policy changes.

### Agency Heads

- Ensure and oversee agency's information technology security program and ensure compliance with the security policy and related standards.
- Ensure agency security policies, procedures and other documents necessary for the security program are developed, implemented, maintained and tested.
- Ensure all agency user of IT resources are trained to follow security policies, standards and procedures.

## CONTACT INFORMATION

For questions about this policy, please contact the OCIO [1].

## REVISION HISTORY

| Date | Action taken |
|---|---|
| December 10, 2014 | Policy adopted. |
| | |

## APPROVING AUTHORITY

/s/ Michael Cockrill — 12/10/2014
State Chief Information Officer — Date
Chair, Technology Services Board

---

Source URL: https://ocio.wa.gov/policies/143-it-security-incident-communication

Links:
[1] http://ofm.wa.gov/ocio/resources/consultants.pdf
[2] https://ocio.wa.gov/policies/143-appendix-us-cert-traffic-light-protocol
[3] http://apps.leg.wa.gov/rcw/default.aspx?cite=42.56.590
[4] https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets