SEC-10
State CIO Adopted: September 12, 2024
TSB Approved: September 12, 2024
Sunset Review: September 12, 2027

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (11)
December 11, 2017
IT Security Incidents
Communications 143
December 10, 2014

IT SECURITY INCIDENT RESPONSE POLICY

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.052 Powers and duties of agency—Application to higher education, legislature, and judiciary.
RCW 43.105.020 (22) "State agency"
RCW 38.52.030 Continuity of Government Operations Preparation
Governor's Directive 13-02 Continuity of Government Operations Preparation

1. **WaTech will provide an Enterprise Incident Response Plan (EIRP) that delineates state and agency responsibilities.**

2. **WaTech will provide a template incident response plan guideline for agencies.**

3. **Agencies must establish, maintain, document, and distribute an agency-level incident response plan (AIRP) that aligns with the EIRP.**

    a. Agencies must keep multiple copies of the AIRP plans online and offline. Offline copies can be physically (printed) or digitally (USB/removable media) stored and must be kept secure. See the SEC-08-02-S Encryption Standard and the SEC-07 Physical and Environmental Protection Policy.

    b. Staff required to execute the plan must have access to both online and offline copies.

    c. Agencies must incorporate Incident Command System (ICS) principles into their incident response processes. See ICS 100, 200, 300 ICS Resource Center (fema.gov).

    d. The agency must redistribute the plan when updated.

4. **At a minimum, the AIRP must address the following:**

    a. Define incident response roles and responsibilities relating to both agency-specific and enterprise incidents.

    b. Assign specific agency incident response roles and responsibilities.

    c. Communication and contact processes that align with the EIRP.

    d. Reference or include Continuity of Operations Plan (COOP), Disaster

Recovery Plan(s) and data backup processes. See SEC-04-01-S Data Backup and Recovery and SEC-12 Disaster Recovery Planning Policy.

e. Escalation procedures that align with EIRP.

f. Staff training, both technical and end user training, to meet incident response responsibilities. See the SEC-03 IT Security and Privacy Awareness Training Policy.

5. **Agencies must incorporate the AIRP in the agency IT Security Program.**

    a. Agencies must exercise the plan annually to test the effectiveness of the plan, the training, and to identify areas for improvement.

    b. Agencies must develop processes to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

6. **Agencies must report cybersecurity incidents to WaTech according to the EIRP.**

7. **WaTech's Security Operations Center (SOC) must investigate agency-reported incidents to confirm the severity, conduct reporting and notification, and coordinate incident management according to the EIRP.**

8. **The State CISO will appoint an Incident Commander who convenes the Enterprise Cybersecurity Incident Response Team (eCIRT) as defined by the EIRP.**

9. **The eCIRT coordinates and approves all communications related to enterprise security incidents according to the EIRP. This includes communications from WaTech and impacted agencies.**

    a. State CISO will notify the state CIO and the Office of Privacy and Data Protection (OPDP) according to the EIRP.

    b. The state CIO will notify the Governor's office that an incident has occurred and may require public notification according to the EIRP.

    c. Agencies will fully cooperate with the Governor's office in support of disclosure of the incident and will coordinate with the eCIRT.

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.
2. SEC-08-02-S Encryption Standard.
3. SEC-07 Physical and Environmental Protection Policy.

4. ICS 100, 200, 300 ICS Resource Center (fema.gov).
5. SEC-01-01-S Data Backup and Recovery Standard.
6. SEC-12 Disaster Recovery Planning.
7. SEC-03 IT Security and Privacy Awareness Training Policy.
8. NIST Cybersecurity Framework Mapping:
    - Respond.Response Planning-1 (RS.RP-1): Response plan is executed during or after an event.
    - Respond.Communications-2 (RS.CO-2): Events are reported consistent with established criteria.
    - Respond.Communications -5 (RS.CO-5): Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.
    - Respond.Analysis-1 (RS.AN-1): Notifications from detection systems are investigated.
    - Respond.Analysis -2 (RS.AN-2): The impact of the incident is understood.
    - Respond.Analysis -3 (RS.AN-3): Forensics are performed.
    - Respond.Analysis -4 (RS.AN-4): Incidents are categorized consistent with response plans.
    - Respond.Mitigation-1 (RS.MI-1): Incidents are contained.
    - Respond.Mitigation-2 (RS.MI-2): Incidents are mitigated.
    - Respond.Improvements-1 (RS.IM-1): Response plans incorporate lessons learned.
    - Respond.Improvements-2 (RS.IM-2): Response strategies are updated.
    - Recover.Communications-1 (RC.CO-1): Public relations are managed.
    - Recover.Communications-2 (RC.CO-2): Reputation after an event is repaired.
    - Recover.Communications-3 (RC.CO-3): Recovery activities are communicated to internal stakeholders and executive and management teams.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.