WaTech
Washington Technology Solutions

Incident Response Policy Background

New, Update or Sunset Review? Response.

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

This policy was developed with a workgroup derived from the Enterprise Security Governance group. The document is informed by the RCW, as well as NIST industry standards.

What is the business case for the policy/standard?

“A failure to plan is planning to fail.” - Attributed to Benjamin Franklin.

This document is necessary for ensuring a coherent and cohesive response to cybersecurity incidents that can cause irreparable harm to critical data and infrastructure.

What are the key objectives of the policy/standard?

- Ensure enterprise framework for incident response actions that affect critical data and infrastructure.
- The enterprise incident response plan will be used as a model by agencies.
- Agencies will create agency-level incident response plans that align to the enterprise incident response plan.

How does policy/standard promote or support alignment with strategies?

This policy supports WaTech’s strategic plan goal for statewide technology leadership by ensuring WaTech is supporting agencies in a cybersecurity incident, especially for high-impact incidents.

What are the implementation considerations?

Agencies will need support to develop their documentation. WaTech will create a template in addition to the model plan to support development of agency incident response plans.

Agencies will also need to support training for employees who will execute the plan in the event of an incident.

How will we know if the policy is successful?

Specific: Agencies will develop and implement an incident response plan tailored to the needs of supported organizations/departments, outlining procedures for identifying, containing, and mitigating cybersecurity incidents. Agencies will support training for all relevant teams.
Measurable: Agencies will achieve a 100% completion rate of incident response plan documentation and training for all relevant internal agency teams.
Achievable: WaTech will provide a template and support for agency policy alignment. Agencies will utilize their plans in the event of an incident and update their plan.
Relevant: Cyber attacks are on the increase, and incidents will happen. Planning in advance is the best way to reduce the impact of cybersecurity incidents.
Timebound: This policy is in effect when adopted. This includes all phases of the incident response lifecycle.
Equitable: This policy aims to consider the needs of all agencies, and in the incident response plan the agencies will be directed to consider the needs of underserved communities when responding to incidents and developing equitable.