WaTech
Washington Technology Solutions

Endpoint Detection and Response Background

New, Update or Sunset Review? Sunset Review. Replaces Section 5.7.

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.

Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability.

Updates to this policy draw from NIST SP 800-83r1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

What is the business case for the policy/standard?

Protecting the state government network from malicious software prevents serious breaches of security including loss of availability, confidentiality, and integrity of state systems and data.

What are the key objectives of the policy/standard?

- Require agencies to implement anti-malware protection and address malware prevention, detection, and removal.
- Require agencies to report endpoint detection response logging information to the state enterprise Security Information and Event Management (SIEM) Service.

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

This standard aligns with WaTech's pillar of "Security, Privacy, and Digital Trust" and with the enterprise IT strategic pillar of Digital Trust.

What are the implementation considerations?

WaTech offers an endpoint detection and response service that agencies may leverage to meet this standard.

How will we know if the policy is successful?

Specific: Agencies will ensure malware detection and prevention software is deployed and kept current on all state-issued devices.
Measurable: Agencies can validate that all devices are running appropriate software. WaTech can measure the number of logs reported to the SIEM.
Achievable: WaTech offers a solution for this, and agencies should already have implemented software.
Relevant: Attempts to breach state security are on the rise due to improved technology leveraged by threat actors.
Timely: This standard is effective when adopted.
Equitable: WaTech offers a solution to ensure all agencies are successful with implementing malware protection.