SEC-04-09-S
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 (5.7)
December 11, 2017

ENDPOINT DETECTION AND RESPONSE STANDARD

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"

1. **Agencies must deploy an Endpoint Detection and Response (EDR) solution on state-issued endpoints and where possible configure reporting into the Enterprise Security Information and Event Management (SIEM) service. See SEC-09-01-S Security Logging Standard.**

    a. Agencies must keep EDR agents and components up to date (N-1 version) on state-issued endpoints. SEC-04-06-S Mobile Device Security Standard provides additional security requirements for devices.

    b. Agencies must document and standardize the deployed EDR's configuration following industry standards and manufacturer's best practices. This includes, but may not be limited to: scanning frequency, inbound and outbound malware detection settings, Host Intrusion configurations, etc.

2. **Agencies must configure the EDR to provide anti-malware protection and address malware prevention, detection, and removal.**

    a. Agencies must implement detection, prevention, and recovery controls to protect against malicious code.

    b. Agencies must examine file transfers, email, and web browser-based traffic for malicious and inappropriate content.

3. **Agencies must set requirements for malware protection for non-state issued endpoints used for work purposes in accordance with the SEC-04-07-S Non-Agency Issued Device Security Standard.**

REFERENCES

1. Definitions of Terms Used in WaTech Policies and Reports
2. SEC-09-01-S Security Logging Standard
3. SEC-04-06-S Mobile Device Security Standard

4. SEC-04-07-S Non-Agency Issued Device Security Standard
5. NIST Cybersecurity Framework Mapping:
    - Protect.Data Security (PR.DS-6): Integrity checking mechanisms are used to verify software, firmware, and information integrity.
    - Protect.Maintenance (PR.MA-2): Remote maintenance of organizational assets is approved , logged, and performed in a manner that prevents unauthorized access.
    - Detect.Security Continuous Monitoring (DE.CM-4): Malicious code is detected.
    - Respond.Analysis (RS.AN-3): Forensics are performed.

CONTACT INFORMATION

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