SEC-09-01-S
State CIO Adopted: April 1, 2024
TSB Approved: Pending
Sunset Review: Pending

Replaces:
IT Security Standard 141.10 (10)
December 11, 2017

WaTech
Washington Technology Solutions

SECURITY LOGGING STANDARD

See Also:
RCW 43.105.450 Office of Cybersecurity
RCW 43.105.054 OCIO Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (22) "State agency"

1. **Agencies must configure their information technology systems and networks to generate security logs (See NIST 800-92 - Guide to Computer Security Log Management).**
   a. Data contained in security logs is considered Category 3 data and is exempt from public records disclosure per RCW 42.56.420.(See the Data Classification Standard.)
   b. Agencies must configure the following systems to log information, exceptions, and user account activity necessary to reconstruct security events:
      i. Security software.
      ii. Antivirus software.
      iii. Firewalls
      iv. Intrusion detection and prevention systems.
      v. Operating systems and servers.
      vi. Workstations.
      vii. Network equipment.
      viii. Applications.
2. **Each log entry must include the following data, where available:**
   a. Account / User ID
   b. Port Number
   c. Type of event

    d. Success or failure of the event

    e. Date and time of the event (timestamp)

    f. Source and Destination IP addresses

3. **Agencies must configure agency security log generation processes to notify agency security administrators in the event of a log generation error. Alerts must be auditable and as close to real time as possible. See the Audit and Accountability Policy.**

4. **Agencies must harden their logging infrastructure according to the Configuration Management Standard.**

5. **Agencies must protect agency security logs from unauthorized access, modification, and deletion.**

6. **Agencies must retain the agency's security logs for at least one year. See Washington Secretary of State's General Records Retention Schedule.**

    a. Agencies must ensure retained security logs are not corrupted.

    b. Agencies may need to meet longer log retention criteria due to Criminal Justice Information Services (CJIS) and Health Insurance Portability and Accountability Act (HIPAA) requirements.

    c. Agencies must develop and document a process to provide for log preservation requests, such as a legal requirement to prevent the alteration and destruction of log records.

REFERENCES

1. NIST Special Publication 800-92, Guide to Computer Security Log Management.
2. SEC-08-01-S Data Classification Standard.
3. SEC-09 Audit and Accountability Policy.
4. SEC-04-03-S Configuration Management Standard.
5. SEC-04-02-S Media Sanitization and Disposal.
6. Definitions of Terms Used in WaTech Policies and Reports.
7. RCW 42.56.420– Security.
8. NIST 800-171 Protecting Controlled by Unclassified Information in Nonfederal Systems and Organizations.
9. Washington Secretary of State's General Records Retention Schedule.

10. NIST Cybersecurity Framework Mapping:
    - PROTECT.PROTECTIVE TECHNOLOGY-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
    - DETECT.ANOMOLIES AND EVENTS-3: Event data are collected and correlated from multiple sources and sensors.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- For risk management document submissions, email the WaTech's Risk Management Mailbox.
- For technical questions or to request a Security Design Review, please email sdr@watech.wa.gov.