SEC-09
State CIO Adopted: November 16, 2023
TSB Approved: November 28, 2023
Sunset Review: November 28, 2026

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (1.6)
December 11, 2017

IT SECURITY AUDIT AND ACCOUNTABILITY POLICY

See Also:
RCW 43.105.450 OCIO Governance
RCW 43.105.054 Office of Cybersecurity
RCW 43.105.205 (3) Higher Ed
RCW 43.105.450 Office of Cybersecurity
About IT Audits | Office of the Washington State Auditor

1. **Agencies must ensure an audit is performed once every three years to determine compliance with WaTech's IT security policies and standards.**

    a. Ensure the audit is approved by a qualified individuals accredited by an authorizing body, such as Information Systems Audit and Control Association (ISACA), Institute of Internal Auditors (IIA), American Institute of Certified Public Accountants (AICPA) or another nationally recognized information technology auditing certification.

    b. Agencies must refer auditors to the State Auditor's Office (SAO) to ensure information security audits are performed in accordance with the SAO's agreed upon procedures.

    c. The auditor must be independent of the agency's IT organization but may be within the agency.

    d. Submit the triennial audit notice of completion to the State Chief Information Security Officer risk management mailbox within thirty calendar days of the final audit report.

    e. Maintain documentation showing the results of the audit according to applicable records retention requirements.

2. **Agencies must respond to IT security audit non-conformities.**

    a. Within three months of the final audit report date, agencies must identify the root causes of their audit findings.

    b. Agencies must document and implement a waiver request according to the Technology Policy and Standards Waiver Request with a plan to correct audit nonconformities and track progress. Agencies must submit this plan to the State Chief Information Security Officer.

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.
2. POL-01-02-PR Technology Policies and Standards Waiver Procedure.
3. NIST Cybersecurity Framework Mapping
    - Identify.Governance-1: Organizational cybersecurity policy is established and communicated.
    - Identify.Governance-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
    - Identify. Supply Chain Risk Management-4: Suppliers and third-party partners are

routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
- Protect.Protective Technology-1 (PR.PT-1): Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.

CONTACTS

- For questions about this standard, please email the policy mailbox.
- For technical questions, please email the risk management mailbox.
- For questions regarding the SAO process, please email SAOITAUDIT@sao.wa.gov.