SEC-01
State CIO Adopted: Dec. 10, 2024
TSB Approved: Dec. 10, 2024
Sunset Review: Dec. 10, 2027

WaTech
Washington Technology Solutions

Replaces:
IT Policy 141
Securing Information Technology Assets
October 1, 2011
IT Standard 141.10 (1.1, 2.1-2.5)
November 13, 2017

WASHINGTON STATE CYBERSECURITY PROGRAM POLICY

See Also:
RCW 43.105.054 WaTech Governance.
RCW 43.105.020 (22) "State agency".
RCW 43.105.052 Powers and duties of agency—Application to higher education, legislature, and judiciary.
RCW 52.105.450 (6, 8) Office of Cybersecurity – Higher education, Judicial, and Legislative
RCW 52.105.450 (3j, 7a) Office of Cybersecurity – Agency IT Security Program
RCW 42.56.420 Security

1. **WaTech will establish enterprise information security programs, policies, and standards to provide the foundation for managing cybersecurity risk and maintaining compliance with applicable laws, regulations, contractual obligations, and alignment with industry standards.**

2. **WaTech and agencies should base information security programs, policies, standards, and technological decisions on information security and architectural principles. See SEC-01-01-G Security Principles Guideline.**

3. **The IT security policies and standards in this chapter apply to the executive branch agencies of the state of Washington, as well as agencies headed by separately elected officials, referred to in this and other policies and standards as "agencies."**

4. **The IT security policies and standards in this chapter apply to any entity using WaTech services in relation to the provided service(s).**

5. **State agencies will adhere to all WaTech policies and standards.**

    a. Institutions of higher education, legislative, and judiciary agencies are not directly subject to Washington state IT security policies and standards but must develop comparable documents appropriate to their respective missions and consistent with the intended outcomes of WaTech's security policies and standards to minimize cyber risks and secure data, systems and infrastructure.

    b. Agencies are responsible for adherence to these IT security policies and standards to protect IT systems and applications whether they are operated by or for an agency, and whether they operate internally on the State Government Network (SGN) or external to the SGN. Examples of environments external to the SGN include the Inter-Governmental Network

(IGN), the Public Government Network (PGN), business partner hosted services, and cloud services.

c. The IT security policies and standards outlined in the security chapter of the Washington State IT policies are the minimum requirements for state agencies. Agencies may create additional policies, standards, and controls based on their specific needs, as long as they do not conflict with the policies and standards in this chapter.

d. WaTech's Office of Cybersecurity (OCS) is responsible for interpreting policies and standards within the security chapter of the Washington State IT Policies. OCS will negotiate the implementation of compensating controls with agencies to ensure cybersecurity risks are reduced to an acceptable level..

e. Non-enforcement of any requirement in this or any information security policy or standard within the Security chapter does not imply consent of non-compliance by WaTech, OCS, or agency management.

6. **Each agency must develop and implement an agency cybersecurity program containing IT security policies, standards, procedures, and all necessary program-related documents.**

a. The agency will review this program at least annually and make appropriate updates after any significant change to its business operations, or information technology environment.

b. Agency Cybersecurity Program documentation must, at a minimum, include:

i. Alignment with the agency's risk management program and strategy.

ii. Clearly identified security objectives for agency systems.

iii. Policies, standards, and procedures in alignment with Washington State enterprise IT policies, standards, and applicable regulatory and contractual obligations.

iv. Details in proportion to the size, complexity, potential risk, and business exposure based on the agency's risk assessment results.

v. Details of the security controls applied to agency systems.

vi. Details, justifications, and waivers from WaTech regarding any deviation from state security policies or standards. POL-01-02-S Technology Policy & Standard Waiver Request Standard.

vii. Records from risk and security assessments and evaluations.

viii. Mechanisms for receiving, documenting, and responding to reported security issues.

7. **Agency heads and CIOs will attest in an annual certification to WaTech that the agency has developed and implemented the agency's Information Technology Security Program and that the program complies with all enterprise information security policies and standards. See POL-01 Technology Policies, Standards, and Procedures Policy.**

8. **Agencies will maintain systems, networks, and applications to minimize risks to:**

    a. **Confidentiality:** Protecting information from unauthorized access and disclosure.

    b. **Integrity:** Confirming that data remains accurate, complete, and unaltered during storage, processing, and transmission.

    c. **Availability:** Systems, networks, and data are accessible to authorized users when needed.

    d. **Compliance:** Adhering to relevant laws, regulations, policies and standards.

    e. **Operational Continuity:** Maintaining the ability to sustain essential functions during and after a cybersecurity incident.

    f. **User Privacy:** Safeguarding personal data and respecting the privacy rights of individuals.

    g. **Reputation:** Protecting the state's reputation by preventing breaches and safeguarding the trust of stakeholders.

    h. **Financial Stability:** Preventing financial losses from cyber-attacks, including direct theft, fraud, or costs associated with recovery and mitigation.

    i. **Intellectual Property:** Securing proprietary information and trade secrets from theft or unauthorized disclosure.

    j. **Third-Party Trust:** Safeguarding that interactions with partners, vendors, and customers are secure, maintaining trust and protecting shared data.

    k. **Equity and Accessibility**: Ensuring fair and equitable treatment in all cybersecurity practices, policies, and procedures, promoting inclusivity and access to secure systems for authorized individuals, regardless of their

background or circumstances. See USER-01 Accessibility Policy and USER-01-01-S Minimum Accessibility Standard.

9. **Organizational users who violate security policies and standards in the security chapter of the Washington State IT policies may be subject to appropriate disciplinary action up to and including discharge, termination of contractual agreements, denial of access to state information assets, and other actions as well as civil and criminal penalties.**

10. **Agencies must provide IT security orientation and supervision of organizational users with access to agency IT assets. Agencies will conduct reference checks and background investigations as required by the agency's IT security program.**

11. **Agencies must include appropriate language in vendor and partner contracts and agreements to ensure alignment with WaTech and agency security policies, standards, and requirements.**

REFERENCES

1. WaTech IT Policies Security Chapter.
2. POL-01-02-S Technology Policy & Standard Waiver Request Standard
3. POL-01 Technology Policies, Standards, and Procedures Policy.
4. Definition of Terms Used in WaTech Policies and Reports.
5. SEC-08-01-S Data Classification Standard.
6. SEC-08 Data Sharing Policy.
7. NIST Cybersecurity Framework Mapping:

- Identify.Asset Management-6 (ID.AM-6): Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.
- Identify.Business Environment-5 (ID.BE-5): Resilience requirements to support delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).
- Identify.Governance-4 (ID.GV-4): Governance and risk management processes address cybersecurity risks.
- Protect. Information Protection Processes and Procedures-7 (PR.IP-7): Protection processes are continuously improved.
- Protect. Information Protection Processes and Procedures-8 (PR.IP-8): Effectiveness of protection technologies is shared with appropriate parties.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- For technical assistance, please email Risk Management.