

USER-02

State CIO Adopted: August 11, 2023

TSB Approved: September 14, 2023

Sunset Review: September 14, 2026



Replaces:
IT Security Standard 141.10 (2.10)
December 11, 2017

ACCEPTABLE USE POLICY

See Also:

RCW [43.105.054](#) WaTech Governance

RCW [43.105.205](#) (3) Higher Ed

RCW [43.105.020](#) (22) "State agency"

RCW 39.26.340 Data Sharing - Contractors

RCW 39.24.240 Data Sharing - Agencies

Fraud Program - Office of the State Auditor

SEC-08 [Data Sharing Policy](#)

SEC-08-01-S [Data Classification Standard](#)

SEC-08-02-S [Encryption Standard](#)

SEC-03 [IT Security and Privacy Awareness Training](#)

SEC-06 [Access Control Policy](#)

- 1. Individual accountability is required when accessing all [Information Technology \(IT\) assets](#) and organization information.**
- 2. Agency information and IT assets are the property of the State of Washington and must be used in conformance with this policy and applicable laws.**
 - a. Agency IT assets are to be used to conduct State of Washington business. Refer to sections 2(b)-Agency approved use and 3-Permitted personal use of state resources of [WAC 292-110-010 - Use of state resources](#) for additional information.
 - b. The following requirements apply to removable storage media:
 - i. Users may not copy agency data onto personal storage media.
 - ii. Unauthorized devices may not be plugged into agency assets.
 - c. Minimal personal use is permitted, provided such use is:
 - i. Consistent with [WAC 292-110-010 - Use of state resources](#).
 - ii. Does not impede the ability of the individual or other users to fulfill the agency's responsibilities and duties, including but not limited to utilization of extensive bandwidth, resource, or storage.
 - iii. Does not compromise the security or integrity of agency IT assets.
 - iv. Agencies may revoke or limit the personal use of state resources privilege at any time.

- d. Users are prohibited from unauthorized changes of IT asset configuration.
- e. Users cannot connect personal devices to the agency network without express permission from agency management.

3. Use of state IT assets constitutes express consent for monitoring and/or inspection of:

- a. Any data users create, access, send, or receive.
- b. Any messages users send or receive.
- c. Any web sites that users access.

4. Access to systems does not guarantee personal privacy for any activity when using such systems. This includes legitimate state purposes, minimal personal use, violations of acceptable use or any other use.

- a. Anyone authorized to access systems expecting privacy for their minimal personal use should not use agency IT assets. See section 4 of [WAC 292-110-010 - Use of State Resources](#).
- b. See the [Mobile Device Security Standard](#) for additional information regarding use of personal devices for official state business.

5. Anyone using agency-issued [endpoints](#) is expected to exercise a reasonable level of protection over those devices.

- a. Endpoints must be used and stored in a manner to prevent unauthorized physical access.
- b. Users must physically secure unattended agency-issued endpoints from unauthorized access and must not leave the item unattended in publicly accessible areas.

6. Agency policies and contracts may restrict access to any websites, domains, or content.

- a. Anyone using agency IT assets to access the intranet, or the internet, must comply with all security policies to protect the confidentiality, integrity, and availability of agency information assets.
- b. The use of unauthorized software for content sharing is prohibited. Unauthorized connection of wireless access points, including cellular devices, to agency networks is prohibited.

7. Agencies reserve the right to monitor agency-issued endpoints and computing

devices.

- a. Agency-issued computing devices are assigned to users to assist them in the performance of their duties. Agencies have the responsibility and right to monitor all aspects of agency IT assets.
- b. Agencies must seize and work with WaTech to inspect any information asset and/or data stored on agency-issued endpoints during the investigation of a security incident or fraudulent activity. Refer additionally to the [IT Security Incident Communication Policy](#).

REFERENCES

1. Link to reference.
2. [Definition of Terms Used in WaTech Policies and Reports](#).
3. [Mobile Device Security Standard \(under development - see 141.10 \(5.8\)\)](#)
4. [WAC 292-110-010 - Use of State Resources](#)
5. [IT Security Incident Communication](#)

CONTACT INFORMATION

- For questions about this policy, please email the [WaTech Policy Mailbox](#).
- For technical security questions or to request a Design Review, please email the [Security Design Review Mailbox](#).