

WaTech

Washington Technology Solutions

MOBILE DEVICE USAGE POLICY

See Also:

RCW [43.105.450](#) Office of Cybersecurity

RCW [40.14.020 \(23\)](#) "State agency"

RCW [40.14.060](#) Destruction, disposition of public records

RCW [43.105.054](#) WaTech Governance

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

RCW [43.105.020](#) (23) "State agency"

NIST [SP 800-124 Rev. 2](#), Guidelines for Managing the Security of Mobile Devices.

1. **Agencies must implement policies and procedures controlling the use of category 3 and above data on agency-issued or agency-approved personal [mobile devices](#). See the [Data Classification Standard](#) [Mobile Device Security Standard](#), and the [Non-Agency Issued Device Security Standard](#). At a minimum, agencies must:**
 - a. Define and document the allowable use of category 3 data or above on mobile devices.
 - b. Review and update their policies and procedures every three years.
 - c. Maintain an escalation process for lost or compromised devices to ensure prompt compliance with all relevant governance requirements.
2. **Agencies must follow the [Mobile Device Security Standard](#) for device configuration requirements.**
3. **Records generated or stored on mobile devices must follow [Secretary of State Agencies Records Retention Schedules](#) and public records policies and laws.**
 - Agencies must [notify the State Auditor's Office \(SAO\)](#) of a lost mobile device according to [RCW 43.09.185](#).
 - Agencies must also follow Office of Financial Management requirements for suspected losses of public funds and property as described in the State Administrative Accounting Manual (SAAM) section [70.75](#).
4. **Agencies must follow the [Media Sanitization and Disposal Standard](#) for agency-owned devices. Any device that is no longer accessible and the sensitivity of data is undetermined, the device is to be considered to contain category 3 data and disposed of accordingly.**
5. **Agencies must address the following at a minimum in their Mobile Device Usage Policy and procedures and communicate that policy to each employee when onboarding, annually, and when revised.**
 - a. Users' basic rights and responsibilities concerning mobile device usage for agency business, including privacy considerations.
 - b. What kinds of mobile devices or solutions (if any) are prohibited.
 - c. What constitutes a public record on a mobile device.

- d. The process by which the agency receives access to public records prepared, owned, used, or retained on mobile devices, including encrypted communications.
- e. User responsibilities for the protection of confidential data, records, and customer information.
- f. Role-specific security measures the user is expected to take to protect the mobile device and the public records stored there from theft, loss, or unauthorized disclosure. See [Mobile Device Security Standard](#).
- g. How to notify the agency if a mobile device is lost, stolen, destroyed, or compromised.

REFERENCES

1. [Data Classification Standard](#).
2. [Mobile Device Security Standard](#).
3. [Non-Agency Issued Device Security Standard](#)
4. [SP 800-124 Rev. 2](#), Guidelines for Managing the Security of Mobile Devices in the Enterprise.
5. [Encryption Standard](#).
6. [Secretary of State Agencies Records Retention Schedules](#).
7. [Reporting Losses of Public Funds or Assets or Other Illegal Activity | Office of the Washington State Auditor](#)
8. [RCW 43.09.185](#).
9. State Administrative Accounting Manual (SAAM) section [70.75](#).
10. [Media Sanitization and Disposal Standard](#).
11. [Definitions of Terms Used in WaTech Policies and Reports](#).
12. NIST Cybersecurity Framework Mapping:
 - a. IDENTIFY.GOVERNANCE-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.
 - b. PROTECT.ASSET CONTROL-3: Remote access is managed.
 - c. PROTECT.DATA SECURITY-2: Data-in-Transit is protected.
 - d. PROTECT.PROTECTIVE TECHNOLOGY-2: Removeable media is protected, and its use restricted according to policy.

CONTACT INFORMATION

- For questions about this policy, please contact the [WaTech Policy Mailbox](#)
- For risk management document submissions, contact the [WaTech's Risk Management Mailbox](#).