USER-03
State CIO Adopted: April 1, 2024
TSB Approved: June 24, 2024
Sunset Review: June 24, 2027

Replaces:
IT Policy 191 Mobile Device Usage
June 12, 2018

MOBILE DEVICE USAGE POLICY

See Also:
RCW 43.105.054 WaTech Governance
RCW 43.105.052 Powers and duties of agency–Application to higher education, legislature, and judiciary.
RCW 43.105.020 (22) "State agency"
RCW 43.105.450 Office of Cybersecurity
RCW 40.14.060 Destruction, disposition of public records
NIST SP 800-124 Rev. 2, Guidelines for Managing the Security of Mobile Devices in the Enterprise.

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 SEC-08-01-S Data Classification Standard SEC-04-06-S Mobile Device Security Standard, and the SEC-04-07-S 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 SEC-04-06-S 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.**

    a. Agencies must notify the State Auditor's Office (SAO) of a lost mobile device according to RCW 43.09.185 - Loss of public funds.

    b. 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 SEC-04-02-S 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. Qualification 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. See SEC-08-02-S Encryption Standard.

   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 SEC-04-06-S Mobile Device Security Standard.

   g. How to notify the agency if a mobile device is lost, stolen, destroyed, or compromised.

REFERENCES

1. Definition of Terms Used in WaTech Policies and Reports.
2. SEC-08-01-S Data Classification Standard.
3. SEC-04-06-S Mobile Device Security Standard.
4. SEC-04-07-S Non-Agency Issued Device Security Standard.
5. Secretary of State Agencies Records Retention Schedules.
6. RCW 43.09.185 - Loss of public funds.
7. SEC-04-02-S Media Sanitization and Disposal Standard.
8. SEC-08-02-S Encryption Standard.
9. NIST Cybersecurity Framework Mapping:
   - IDENTIFY.GOVERNANCE-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.

- PROTECT.ASSET CONTROL-3: Remote access is managed.
- PROTECT.DATA SECURITY-2: Data-in-Transit is protected.
- PROTECT.PROTECTIVE TECHNOLOGY-2: Removeable media is protected, and its use restricted according to policy.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.