SEC-04-07-S
State CIO Adopted: April 1 2024
TSB Approved: June 24. 2024
Sunset Review: June 24, 2027

Replaces:
NEW

WaTech
Washington Technology Solutions

NON-AGENCY ISSUED DEVICE SECURITY STANDARD

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
USER-02 Mobile Device Usage Policy
SEC-04-06-S Mobile Device Security Standard
NIST Mobile Device Security
NIST Guidelines for Managing the Security of Mobile Devices in the Enterprise.
LEP Mobile Device Policy.
Purdue University Mobile Devices Security Best Practices.
IRS 10.8.26 Wireless & Mobile Device Security Policy

1. **Agencies are strongly discouraged against allowing the use of non-agency owned (known as 'bring your own device' or BYOD) and managed computers for work purposes. If agencies decide to allow this option, agencies must:**

    a. Determine what non-agency owned computers technical support it will provide.

    b. Ensure they identify, document, and control the asset.

    c. Implement controls to prevent access to the SGN network.

    d. Ensure antivirus, software and operating system versions and patching are up to date.

    e. Microsoft 365 services may be accessed with the following controls outside of a Mobile Device Management (MDM) or Enterprise Mobility Management (EMM):

        i. Conditional access policies must prevent users from downloading data. See SEC-06 Access Control Policy.

        ii. Multi-factor authentication must be employed if remote.

2. **If employees are using non-agency owned devices for work purposes, agencies must require MDM or EMM software enrollment for mobile devices.**

a. Agencies must document processes for wiping devices and removing the MDM or EMM software.

b. Microsoft 365 services are controlled by enterprise-level Conditional Access Policies, and may be accessed with the following controls outside of an MDM or EMM:

i. Multi-factor authentication must be employed.

ii. Conditional access policies must prevent users from downloading data.

iii. Microsoft's Authenticator application must be installed.

iv. Users must utilize a pin to access the device.

3. **Agencies must require a written agreement for using personal devices for state business.**

a. End-users must acknowledge in writing that state records, such as text messages or pictures, on personal devices, are publicly disclosable and subject to records retention requirements, and that the device must be made available as required. See the Secretary of State Records Retention Schedules.

REFERENCES

1. Definitions of Terms Used in WaTech Policies and Reports.
2. SEC-06 Access Control Policy.
3. Secretary of State Records Retention Schedules.
4. 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 email the WaTech Policy Mailbox.
- To request an MDM or EMM solution, please file a ServiceNow request.