WaTech
Washington Technology Solutions

MOBILE DEVICE SECURITY STANDARD

See Also:
RCW 43.105.450 Office of Cybersecurity
RCW 43.105.054 WaTech Governance
RCW 43.105.205 (3) Higher Ed
RCW 43.105.020 (23) "State agency"
USER-02 Mobile Device Usage Policy
SEC-04-07-S Non-Agency Device Security Standard
NIST Mobile Device Security
NIST SP 800-124 Rev. 2, Guidelines for Managing the Security of Mobile Devices
Limited English Proficiency (LEP) Mobile Device Policy (Example)
Purdue University Mobile Devices Security Best Practices.
IRS 10.8.26 Wireless & Mobile Device Security Policy
SEC-04-02-S Media Sanitization and Disposal Standard

1. **Agencies must select appropriate controls and communicate them through their mobile device policies and procedures.**

   a. Agencies must encrypt category 3 data or above (See the SEC-08-01-S Data Classification Standard) on mobile devices per the SEC-08-02-S Encryption Standard.

   b. Agencies must implement controls to prevent the auto-launching of non- agency approved applications at the device's start-up. Agencies must perform and document a business criticality assessment and a risk assessment for any auto launch application.

   c. Agencies must train users on 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.

   d. Agencies must implement authentication requirements:

      i. Require device authentication mechanism to access the device, such as a PIN, password, or biometric.

      ii. Require application or network access via Multi-factor Authentication (MFA) according to the Securing IT Assets 141.10 (6.3) Identification and Authentication Standard.

      iii. For devices not assigned to a specific user where a PIN and MFA is not feasible, agencies must document mitigating controls.

2. **Agencies must ensure that all mobile solutions used for state business are equipped with up-to-date, currently patched WaTech approved Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) software.**

   a. Synchronization is controlled by the agency MDM or EMM.

   b. Agencies must restrict app store downloads for devices used for agency business.

3. **Mobile operating systems and applications must be currently supported by the vendor and the agency must ensure they are kept up to date. See**

the **SEC-04-03-S Configuration Management Standard**.

4. **Agencies must regularly monitor and maintain mobile device security. This may include but is not limited to:**

    a. Conducting and documenting threat analysis for mobile devices.

    b. Employing enterprise threat defense, mobile application vetting, and other enterprise mobile security technologies.

REFERENCES

1. SEC-08-01-S Data Classification Standard.
2. SEC-08-02-S Encryption Standard.
3. Securing IT Assets 141.10 (6.3) Identification and Authentication Standard.
4. Definitions of Terms Used in WaTech Policies and Reports.
5. SEC-04-03-S Configuration Management Standard.
6. Secretary of State Agencies Records Retention Schedules.
7. NIST Cybersecurity Framework Mapping:
    - PROTECT.AWARENESS TRAINING-1: All users are informed and trained.
    - PROTECT.ACCESS 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.
    - DETECT.SECURITY CONTINUOUS MONITORING-5: Unauthorized mobile code is detected.

CONTACT INFORMATION

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