SEC-06-02-S
State CIO Adopted: November 16, 2023
TSB Approved: November 28, 2023
Sunset Review: November 28, 2026

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 section 6.4
November 13, 2017

REMOTE ACCESS STANDARD

See Also:
RCW 43.105.450 Office of Cybersecurity
RCW 43.105.054 OCIO Governance
RCW 43.105.205 (3) Higher Ed

1. **Agencies must review and approve requests for remote access to any resource on the agency's network. See the 141.10 (6.3) Identification and Authentication Standard.**
2. **Agencies must use WaTech-approved solutions and/or integrations when remotely accessing agency resources and services on the State Government Network (SGN) and internet.**

    a. Includes the state's common remote access services to access the SGN. See WaTech Services Catalog.

    b. Includes internet accessible agency systems, such as Software as a Service (SaaS) or vendor-hosted solutions, not accessed through the state's common remote access services.

    c. Includes remote connections approved by WaTech as part of a Security Design Review.

    d. For service accounts, see the Access Control Policy.

3. **WaTech's Office of Cybersecurity (OCS) must approve all split tunneling destinations. WaTech OCS will evaluate the deployment use case.**
4. **Agencies must conform to the principle of least privilege when configuring their remote access controls. This limits the resources to which access is granted.**
5. **Only agency-owned or approved devices are permitted to use the state's common remote access services such as Internet Protocol Security (IPsec) or Secure Sockets Layer Virtual Private Network (SSL VPN). See the Mobile Device Usage Policy and 141.10 (5.8) Mobile Device Security Standard.**
6. **Agencies and WaTech must monitor for unauthorized remote connections and other anomalous activity and take appropriate incident response action as per the Cyber Incident Response Plan.**

    a. Agencies must ensure remote access sessions and failures are logged according to the 141.10 (10) - Security Logging Standard.

REFERENCES

1. 141.10 (6.3) Identification and Authentication Standard
2. Mobile Device Usage Policy.
3. 141.10 (5.8) - Mobile Device Security Standard.
4. Cyber Incident Response Plan (under development).
5. 141.10 (10) - Security Logging Standard.
6. Configuration Management Standard.
7. NIST 800-46, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

8. Definitions of Terms Used in WaTech Policies and Reports

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox
- For risk management document submissions, email the WaTech Risk Management Mailbox.
- For technical questions or to request a Security Design Review, please email sdr@watech.wa.gov.