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

Replaces:
IT Security Standard 141.10 (6.4)
December 11, 2017

REMOTE ACCESS 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
SEC-04-03-S Configuration Management Standard
NIST 800-46, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

1. **Agencies must review and approve requests for remote access to any resource on the agency's network. See 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's 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 (SDR).

    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 USER-03 Mobile**

Device Usage Policy, SEC-04-06-S Mobile Device Security Standard, and SEC-04-07-S Non-Agency Issued 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 Enterprise Incident Response Plan.**

7. **Agencies must ensure remote access sessions and failures are logged according to the SEC-09-01-S Security Logging Standard.**

REFERENCES

1. Definitions of Terms Used in WaTech Policies and Reports.
2. 141.10 (6.3) Identification and Authentication Standard.
3. WaTech's Services Catalog.
4. USER-03 Mobile Device Usage Policy.
5. SEC-04-06-S Mobile Device Security Standard.
6. SEC-04-07-S Non-Agency Issued Device Security Standard.
7. Enterprise Incident Response Plan - See Contact Information.
8. SEC-09-01-S Security Logging Standard.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- For technical questions or information about the Enterprise Incident Response Plan, please email the WaTech Risk Management Mailbox.
- To request a Security Design Review (SDR), please submit a ticket through our Customer Portal.