WaTech
Washington Technology Solutions

Remote Access Standard Background

New, Update or Sunset Review? New.

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

The 2017 version of OCIO 141.10 addresses remote access at a high level. This new standard includes content from NIST 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.

What is the business case for the policy/standard?

This standard ensures accountability and the implementation of controls for remote access to the State Government Network and the information assets within.

What are the key objectives of the policy/standard?

The key objective of this standard is to establish consistent practices to enable agency staff to access the State Government Network while denying or limiting the access of unauthorized activities.

How does policy/standard promote or support alignment with strategies?

Strategic Planning | Washington Technology Solutions
This policy supports efficient and accountable government by ensuring agencies are managing IT resources comprehensively.

What are the implementation considerations?

Agencies will configure their remote access solution in accordance with this standard.

How will we know if the policy is successful?

Specific: Agencies will only allow authorized access to resources on the agency's network.
Measurable: Analysis of the remote connection logs collected by the Office of Cybersecurity and host agencies will evidence compliance.
Achievable: Agencies will be able to demonstrate the approval request process and their configuration files demonstrating least privilege.

Relevant: Limiting or denying access to unauthorized activities is a key component of asset protection.
Timebound: Agencies will update their processes and documentation in preparation for audits every three years including compensating controls for those not yet in place.
Equitable: Agreed upon procedures ensure that every audit is run the same way for consistency regardless of the agency.

SEC-05-02-S
State CIO Adopted:
TSB Approved:

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10
sections 6.4

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
RCW 43.105.020 (22) "State agency"

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.**
   a. 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. Draft: 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 contact the WaTech Policy Mailbox.
- For risk management document submissions, contact the WaTech's Risk Management Mailbox.
- For technical questions or to request a Security Design Review, please contact sdr@watech.wa.gov.