SEC-04-05-S
State CIO Adopted: May 28, 2024
TSB Approved: June 24, 2024
Sunset Review: June 24, 2027

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (5.2-5.4)
December 11, 2017

NETWORK 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
RCW 43.41.391 K-20 Network
SEC-04-04-S Firewall Standard
SEC-11-01-S Risk Assessment Standard
NIST SP 800-215 Guide to a Secure Enterprise Network Landscape
Center for Information Security (CIS) Control List

1. **Agencies must establish network security controls to manage and mitigate the risks associated with network connections with layered security protections.**

2. **Agencies are encouraged to align network security controls with National Institute of Standards and Technology (NIST) SP 800-207, Zero Trust Architecture.**

3. **Agencies must establish and maintain network architecture diagrams and other network system documentation. Agencies must review and update documentation annually, or when significant architectural changes occur.**

4. **Agencies must implement controls to protect segments and individual assets within each segment.**

    a. Disable remote communications where no business need exists.

    b. Hide internal addresses from exposure on the Internet as necessitated by the risk and complexity of the system.

    c. Implement controls to prevent unauthorized computer connections and information flows through methods such as:

        i. Authentication of routing protocols.

        ii. Ingress filtering at network edge locations.

        iii. Internal route filtering.

        iv. Routing protocols are enabled only on necessary interfaces.

v. Restrict routing updates on access ports.

5. **Agencies must manage infrastructure to support network security by:**

   a. Ensuring network infrastructure is kept up to date per the SEC-11-02-S Vulnerability Management Standard.

   b. Ensuring that network security solutions are capable of blocking connections to known malicious domains or websites by using either:

      i. Domain Name Service (DNS) filtering, or

      ii. Uniform Resource Locator (URL) filtering.

   c. Performing traffic filtering between network segments, where appropriate.

6. **WaTech must support enterprise-wide time sources following Network Time Protocol (NTP) with a primary and backup enterprise time sources.**

   a. WaTech will block all other NTP traffic at the perimeter.

   b. Agencies must synchronize all agency assets with WaTech's established enterprise time sources.

7. **Agencies must take the following security precautions for network assets:**

   a. Establish and maintain a secure configuration process for network devices based on the SEC-04-03-S Configuration Management Standard.

   b. Define and implement network device hardening standards with minimum security baselines, including business justification for use of all services, protocols and ports allowed for system components, specifically security features implemented for those protocols considered to be unsecure e.g., File Transfer Protocol (FTP), Telnet, POP3, IMAP and Simple Network Management Protocol (SNMP).

8. **Agencies with assets connected to the State Government Network (SGN) must:**
   a. Prohibit direct public access from the Internet to any internal system.

   a. Use a WaTech-Managed security layer. The WaTech-managed security layer includes, but is not limited to firewalls, intrusion detection systems, proxy servers, security gateways, Virtual Private Network (VPN), and other security and monitoring systems as deemed necessary by WaTech to protect the integrity of the SGN.

b. Agencies must encrypt Internet traffic according to the SEC-08-02-S Encryption Standard.

9. **Agency IT networks that do not connect to the SGN must use a WaTech-approved security layer to mitigate threats and risks appropriate to the network traffic and data classification. See** SEC-08-01-S Data Classification Standard.

10. **Agencies must obtain WaTech approval for wireless network configuration through a Security Design Review. Agencies are responsible for the secure deployment of wireless networks:**

    a. The agency IT security program documentation must address the use of wireless technologies.

    b. Change wireless vendor defaults including but not limited to pre-shared keys and passwords.

    c. Monitor for unauthorized wireless assets as defined in the agency security program.

    d. Securely segment wireless access point connections from the Internet.

    e. Wireless network deployments that extend their Local Area Networks (LANs) for organizational access must use:

        i. Wireless Protected Access 2 Enterprise (WPA2 Enterprise) or its successors for authentication and encryption.

        ii. Wireless traffic requiring connection to the SGN must be securely segmented, encapsulated or tunneled over shared infrastructure.

    f. Authenticated guest wireless network deployments that do not extend the agency's local area network (LAN) or connect to the SGN must use:

        i. Authentication and encryption controls that are appropriate for the environment.

        ii. Secure segmentation to isolate guest and agency LAN communication.

    g. Open public or unauthenticated wireless network deployments must:

        i. Utilize a dedicated non-state internet service provider,

ii. Must not or traverse infrastructure components that connect to the agency network or SGN; and

iii. Access to the SGN over public access requires the use of remote access services. See the SEC-06-02-S Remote Access Standard.

11. **If wireless networks are prohibited, the agency IT security program documentation must define how this is periodically verified and enforced.**

12. **Agencies must address the collection, review, and retention of audit logs for enterprise assets. See the SEC-09-01-S Security Logging Standard.**

REFERENCES

1. Definitions of Terms Used in WaTech Policies and Reports.
2. SP 800-207, Zero Trust Architecture CSRC.
3. SEC-11-02-S Vulnerability Management Standard
4. SEC-04-03-S Configuration Management Standard.
5. SEC-08-02-S Encryption Standard.
6. SEC-08-01-S Data Classification Standard.
7. SEC-06-02-S Remote Access Standard
8. SEC-09-01-S Security Logging Standard
9. NIST Cybersecurity Framework Mapping:
   - Protect.Identity Management, Authentication and Access Control-5 (PR.AC-5): Network integrity is protected (e.g., network segregation, network segmentation)
   - Protect.Protective Technology-4 (PR.PT-4): Communications and control networks are protected
   - Detect.Anomalies and Events-1 (DE.AE-1): A baseline of network operations and expected data flows for users and systems is established and managed

CONTACT INFORMATION

For questions about this policy, please email the WaTech Policy Mailbox.