SEC-07
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 (3)
December 11, 2017

PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY

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"
NIST 800-53 - Security and Privacy Controls for Information Systems and Organizations.

1. **Agencies must establish roles responsible for defining, documenting, managing, maintaining, monitoring, and testing physical and environmental controls within controlled areas managed by the agency.**

2. **Agencies must document the specific location of agency-managed IT equipment.**

3. **Agencies must restrict physical access to digital and non-digital media and agency-managed IT equipment to authorized individuals only.**

    a. Agencies must document policies and procedures for media and equipment requiring restricted access, users authorized to access area contents, and the specific measures taken to restrict access.

    b. Agencies must issue authorization credentials (e.g., badges) to users accessing a restricted area.

        i. Agencies must inspect the user's photographic identification credentials during the authorization process.

        ii. The level of access provided to each user must not exceed the level of access required to complete the user's job responsibilities.

        iii. Agencies must review and approve access levels prior to granting them to a user.

        iv. Everyone within either an agency location, or another location housing agency-managed IT equipment, must display either an agency-issued identification badge or a current visitor badge.

        v. Agencies must inventory and secure keys, combinations, and other physical access devices to prevent unauthorized access to

agency locations and assets. Agencies must review and update this inventory no less than annually.

A. Agencies must retrieve access mechanisms from users during the user off-boarding process.

B. Agencies must change compromised access mechanisms or combinations to secured areas.

c. Agencies must review and approve location access lists and authorization credentials at least quarterly.

4. **Agencies must monitor physical access to the agency's controlled location(s) where information systems are housed to detect and respond to physical security incidents.**

    a. Agencies must configure monitoring controls to generate an alert in response to a physical security breach.

    b. Agencies must review physical access logs at least monthly.

    c. Agencies must document procedures detailing their response to physical access incidents.

    d. Agencies must investigate physical security violations or suspicious activity in accordance with RCW 43.105.450. 3.d. Office of cybersecurity notify WaTech's Security Operations Center via the Service Portal of incidents that may:

        a. Impact multiple agencies,

        b. Impact more than 10,000 citizens,

        c. Involve a nation state actor, or

        d. Are likely to be in the public domain.

    e. Agencies must report incidents that occur in controlled areas on the capital campus to DES Capitol Security and Visitors Services (CSVS).

5. **Controlled location(s) housing agency-managed IT equipment supporting agency mission critical functions must maintain a visitor log.**

    a. Visitor access records must include at least the following information:

        i. Name and organization of the visitor.

ii. Verification of picture ID.

iii. Data of access.

iv. Time of entry and departure.

v. Purpose of visit.

vi. Name of the person visited.

b. Agencies must review visitor access logs at least monthly.

c. Anomalies in visitor access must be reported to the person responsible for the location's security.

d. Agencies must maintain visitor access records per their retention policies.

6. **Agencies must protect agency-managed power equipment and cabling for information systems from damage and destruction.**

    a. This requirement is optional for low-risk information systems. See SEC-11-02-S Information Security Risk Assessment Standard.

    b. Power back-up solutions should be considered.

7. **Locations housing agency-managed IT equipment must provide the capability of shutting off power to information systems.**

    a. This requirement is optional for low-risk information systems.

    b. Shutdown procedures must have clearly defined controls and procedures to enable an orderly shutdown of computing resources in the event of a prolonged power failure and be documented and distributed to the personnel responsible for the shutdown process.

8. **Agencies must protect critical information technology systems from damage and data loss by installing and routinely testing a source of continuous power.**

    a. This requirement is optional for low-risk information systems.

    b. Continuous power must be provided for mission-critical information assets through battery-operated uninterrupted power supply (UPS) protection. Consideration for generator backup may be contemplated if risk assessments warrant higher levels of protection.

    c. Where possible, emergency power off (EPO) switches must be clearly labeled and located near emergency exits in equipment rooms to facilitate

rapid power down.

9. **Agencies must ensure emergency lighting exists in the locations which house active and operational agency-managed IT equipment.**

10. **Agencies must ensure that locations containing information systems such as data centers, server rooms, and network closets implement controls to monitor, alert, and log fires and smoke.**

11. **Agencies must ensure that all data centers provide and maintain environmental controls to prevent fluctuations potentially harmful to equipment. This includes all cloud vendor solutions. See EA-02-03-S Data Center Investments.**

12. **Agencies must ensure that controlled locations containing information systems such as data centers, server rooms, and network closets implement controls to prevent water damage.**

13. **Agencies must ensure that access from delivery areas to spaces that house information systems enforce authorizations for entry and exit.**

    a. Delivery and removal of assets from agency and state locations must be authorized, monitored, and controlled. Asset location and movement must be monitored so long as asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. See SEC-04 Asset Management Policy. See USER-03 Mobile Device Usage Policy.

14. **Agencies that house data subject to third party compliance requirements, such as CJIS, HIPAA, or IRS publication 1075 must comply with the relevant physical security requirements.**

REFERENCES

1. Definition of Terms Used in Policies and Reports.
2. RCW 43.105.450. 3.d. Office of cybersecurity.
3. SEC-11-02-S Information Security Risk Assessment Standard.
4. EA-02-03-S Data Center Investments.
5. SEC-04 Asset Management Policy.
6. USER-03 Mobile Device Usage Policy.
7. CJIS.
8. HIPAA.
9. IRS publication 1075.

10. NIST Cybersecurity Framework Mapping:

- PROTECT.ACCESS-2: Physical access to assets is managed and protected
- PROTECT.AWARENESS TRAINING-5: Physical and cybersecurity personnel understand the roles and responsibilities
- PROTECT.INFORMATION PROTECT PROCESS AND PROCEDURES-5: Policy and regulations regarding the physical operating environment for organizational assets
- DETECT.SECURITY CONTINUOUS MONITORING-2: The physical environment is monitored to detect potential cybersecurity events.

CONTACT INFORMATION

- For questions about this policy, please email the WaTech Policy Mailbox.
- To contact the Security Operations Center, submit a Service Portal request.