WaTech
Washington Technology Solutions

Physical and Environmental Protection Policy Background

New, Update or Sunset Review? Sunset Review.

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.

This standard expands on and replaces the current 141.10 (3) requirements. Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability.

Updates to this policy draw from the GSA procedural guide CIO-IT Security-12-64 Physical and Environmental Protection (PE) which is based on NIST SP 800-53.

What is the business case for the policy/standard?

- Physical and environmental security must be commensurate with the risks, threats, and vulnerabilities unique to IT assets and their physical site, and geographic location.
- Physical and environmental security are essential controls to ensure agencies can conduct state business safely and with the assurance of the confidentiality, integrity, and availability of state information.

What are the key objectives of the policy/standard?

- Establish the requirements for mitigating the risks from physical security and environmental threats through the establishment of effective physical security and environmental controls.
- Establish requirements for physical security controls for State and agency data centers and information technology (IT) resources within or external to those data centers.

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 need to engage with facility management in cases of joint tenancy and will need to consider compensating controls when the modifications are not possible due to lease restriction or other limitations.
- Agencies will need update their procedures and documentation to align with new technologies on the premises both assets and protective measures.

How will we know if the policy is successful?

Specific: Agencies have documentation people, processes, and technology responsible for the physical and environmental controls within controlled areas.
Measurable: Agencies will use centralized inventories to understand the agency's IT profile and support a secure environment.
Achievable: Agencies will be able to produce a documented plan to resolve deficiencies.
Relevant: Documentation is available for disaster preparedness, business continuity, and other related exercises.
Timebound: Agencies maintain their documentation when changes happen and ensure they are up to date for audits every three years.
Equitable: Agreed upon procedures ensure that every audit is run the same way for consistency regardless of the agency.

SEC-07
State CIO Adopted:
TSB Approved:
Sunset Review:

WaTech
Washington Technology Solutions

Replaces:
IT Security Standard 141.10 (3)
December 11, 2017

PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY

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 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.

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

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

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

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

            D. 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.

            E. 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.

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

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

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

c. Controlled areas must be subject to additional entry controls such as locks, proximity card readers or biometric identification. Agencies must restrict physical access by controlling entry and exit to the location.

d. Agencies must authorize in writing duplication of access mechanisms (card keys and secure keys).

2. **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).

3. **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.

4. **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 the Risk Assessment Standard.

    b. Power back-up solutions should be considered.

5. **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.

6. **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.

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

8. **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.**

9. **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 Data Center Investments.**

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

11. **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 Asset Management Policy. See Mobile Device Usage Policy.

12. **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. NIST 800-53 - Security and Privacy Controls for Information Systems and Organizations
2. Physical and Environmental Protection Policy
3. CJIS
4. HIPAA
5. IRS publication 1075
6. Asset Management Policy
7. Mobile Device Usage Policy
8. 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, utilize the Service Portal.