Physical Security Policy

Effective Date: January 06, 2025	**Category:** Security
Scheduled Review: September 30, 2026	**Supersedes:** ITP-SEC029

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Purpose

This Information Technology Policy (ITP) establishes access controls and facility penetration testing requirements to ensure that Commonwealth Information Technology (IT) facilities and resources are protected by physical security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

3. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this policy as outlined herein.

4. Policy

For definitions found within this document, refer to the *IT Policy Glossary*.

All IT facilities and resources, whether Commonwealth owned or managed, or owned, hosted, or managed by a contracted third-party vendor shall be physically protected in proportion to their criticality or functional importance. IT facilities and resources include:

- Data centers
- Computer rooms
- Telephone closets
- Network routers
- Hub rooms
- Voicemail system rooms
- Similar areas containing IT resources

Protection measures shall include:

- Designated limited access areas that are separated and locked.
- Environmental controls to ensure operating conditions are within specifications for

equipment located within the confines of the area.
- Environmental and safety monitoring devices to ensure compliance with regulations or statutory requirements.
- Inspections on a regular basis to ensure compliance with health, safety, fire, security, and maintenance requirements.
- Documented procedures in place to provide immediate access to IT facilities and resources by fire, safety, and other emergency personnel in the case of an emergency.

4.1 Access Control

At a minimum, agencies shall ensure the access control requirements and restrictions in the following sections are implemented for IT facilities and resources.

4.1.1 Access Control Requirements

- Develop and maintain a list of individuals approved to authorize access to IT facilities and resources.
- Determine a process for granting door keys or access cards for IT facilities and resources. This process shall include the designation of an approved person responsible for providing such access to the facility or room.
- Access cards or keys shall not be shared or loaned to others.
- Non-authorized employees, business partners, and citizen visitors may be granted temporary access via verbal or signed orders when conditions require their immediate access, or visitor access is approved. These individuals:
  - Shall be recorded in the facility sign-in logs. This log will have the minimal visitor responsibilities associated with accessing the facility on each page or otherwise prominently displayed.
  - Shall be issued a temporary identification badge and are required to wear it openly.
  - Shall be supervised at all times while in restricted areas by an individual with authorized access to the IT facilities andresources.
- Designate a responsible party to review access records and visitor logs. These reviews shall be conducted at least once every three months. The reviewer shall:
  - Investigate any unusual access.
  - Remove access privileges for individuals who no longer require right of entry.
- Access records and sign-in logs shall be maintained and archived for routine review for a minimum of one year.

4.1.2 Access Control Restrictions

- Restrict access to IT facilities and resources to only authorized persons.
- No one shall be permitted to enter a controlled-access facility, area, or room without being authenticated and having privileges verified.

4.2 Facility Penetration Testing

Agencies conducting penetration testing of physical access points shall ensure the following steps are followed prior to the start of testing:

- Establish and document rules of engagement:
  - Agreed upon time frame to conduct testing.
  - Preferred communication methods for engagement.
  - Previously known vulnerabilities, and potential concerns or issues that could arise during or should be known for testing.
  - Whether to notify business of exploitations during testing. Does the agency want to enact incident response procedures as part of testing?
  - Procedures if sensitive or confidential data is compromised during testing.
  - Network connectivity requirements, if applicable as part of testing.
- Risks must be identified, understood, and accepted prior to the start of testing.
- Notification of test dates must be provided and approved by the appropriate agency leadership. At a minimum this shall include, Chief Information Officer (CIO), Chief Technology Officer (CTO), and Information Security Officer (ISO).
- Notification shall be provided to Capitol Police and Department of General Services Building Manager (DGS) for DGS managed facilities. A list of DGS managed facilities along with their respective building managers can be found on the **DGS Managed Facilities** webpage. Local law enforcement shall be provided notification for all Commonwealth leased or third-party facilities (via a non-emergency contact number/method).
- A test plan shall be submitted to the Commonwealth Chief Information Security Officer (CISO) at **RA-CISO@pa.gov** at least five (5) business days prior to planned start of testing. The test plan shall include:
  - Types of tests to be performed.
  - How testing will be performed.
  - What will be examined and/or tested.
- An Executive Summary of findings must be submitted to the CISO for review after completing the test.

5. Contact

Questions or comments may be directed via email to OA, IT Policy.

6. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the enterprise IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

7. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document