Information Technology Policy

Physical Security Policy for IT Resources

Number
ITP-SEC029

Effective Date
June 21, 2007

Category
Security

Supersedes
None

Contact
RA-ITCentral@pa.gov

Scheduled Review
May 2025

1. Purpose

This Information Technology Policy (ITP) establishes requirements for access controls 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. Additionally, this policy establishes guidance on facility penetration testing that can identify vulnerabilities within the operating environments of IT facilities or resources and be utilized to remediate or improve physical security controls.

Commonwealth agencies have physical access to IT facilities and resources as described below. Agencies shall take great care in physically securing IT facilities and resources to ensure the integrity of their systems and networks.

2. Scope

This ITP 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 ITP as outlined in the Responsibilities section.

3. Definitions

Facility Penetration Testing: An attempt through testing to bypass or circumvent implemented security controls associated with the physical access of a facility.

4. Policy

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 and resources.
- 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 rules of engagement and document:
  - 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 5 business day 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 the test has completed.

5. Responsibilities

5.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

5.2 Third-party vendors, licensors, contractors, or suppliers shall:

- Implement policies and practices to ensure the protection of physical facilities and appropriate screening for facility access for any IT facility or resource hosting Commonwealth data.
- Ensure their personnel cooperates with Commonwealth worksite requirements, which includes providing information for Commonwealth badging and being escorted. Contractors and Commonwealth approved subcontractors who do not have a Commonwealth badge, shall always display their company identification badge while on Commonwealth premises. The Commonwealth reserves the

right to request additional photo identification from contractor and subcontractor personnel.

- Document an inventory of items (such as tools and equipment) being brought onto the Commonwealth worksites, and submit to a physical search at Commonwealth worksites which have this requirement for persons entering their premises such as the State Police or Department of Corrections. Ensure contractor and subcontractor personnel always have a list of tools being brought onto a site and are prepared to present the list to a Commonwealth employee upon arrival, as well as present the tools or equipment for inspection. Before leaving the worksite, contractor or subcontractor personnel will present the list and the tools or equipment for inspection and may be searched by Commonwealth staff, or a correctional or police officer.
- Restrict access to their IT facilities and resources only to authorized persons.
- Ensure their IT facilities and resources hosting or accessing Commonwealth data designate a certified party to review access records and visitor logs in accordance with this ITP and any applicable legislation.
- Ensure their IT facilities and resources hosting or accessing Commonwealth data are physically protected in proportion to the data or application's criticality or functional importance.
- Ensure procedures in Section 4.2 are adhered to for any Facility Penetration Testing involving IT facilities that host or manage Commonwealth data or resources.

6. Related ITPs/Other References

- Definitions of associated terms of this policy are published on the Office of Administration's public portal: *http://www.oa.pa.gov/Policies/Pages/Glossary.aspx*
- Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: *http://www.oa.pa.gov/Policies/Pages/default.aspx*
- *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *DGS Managed Facilities*

7. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

8. Publication Version Control

It is the Authorized User's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication shall be directed to RA-ITCentral@pa.gov.

9. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver shall be submitted via the enterprise IT policy waiver process. Refer to *ITP-BUS004, IT Policy Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	06/21/2007	Base Policy	N/A
Revision	04/02/2014	ITP Reformat	N/A
Revision	06/08/2021	• ITP Template • Added third-party vendors to Scope and Responsibilities • Added Related ITP Section • Added Exemption Section	N/A
Revision	09/19/2022	• ITP Refresh • Added third party vendor requirements to Responsibilities section from OPD-SEC000B.	N/A
Revision	05/14/2024	• Purpose expanded to include facility penetration testing. • Scope updated based on connection to Commonwealth network and aligns third party vendor requirement to Responsibilities section. • Definitions section added, with definition for Facility Penetration Testing. • Policy language organized and groups into relevant topics, general policy, access control (requirements/restrictions), facility penetration testing. • Added requirement for list of individuals approved to authorize access to IT facilities and resources. • Section 4.2 Facility Penetration Testing added along with policy language/requirements. • Third party vendor responsibilities updated to include requirement around Facility Penetration testing.	Revised IT Policy Redline <05/14/2024>