# 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**
September 2023

## 1. Purpose

This Information Technology Policy (ITP) establishes an information security policy 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.

Commonwealth agencies have physical access to IT facilities and resources such as servers, tape libraries, and communication closets. 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 (hereinafter referred to as "agencies"). Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP that are applicable to the products and services provided to the Commonwealth.

## 3. Policy

IT facilities and resources include data centers, computer rooms, telephone closets, network routers, hub rooms, voicemail system rooms, and similar areas containing IT facilities and resources. These facilities and resources could be commonwealth owned or managed or be owned, hosted, or managed by a contracted third-party supplier. All IT facilities and resources shall be physically protected in proportion to the criticality or functional importance.

Protection measures shall include:

- Separated, locked, and designated as limited access areas.

- Environmentally controlled to ensure operating conditions are within specifications for equipment located within the confines of the area.
- Equipped with environmental and safety monitoring devices to ensure compliance with regulated or statutory requirements.
- Inspected on a regular basis to ensure compliance with health, safety, fire, security, and maintenance requirements.

The following restrictions and requirements shall be placed on IT facilities and resources:

- Restrict access to IT facilities and resources to only authorized persons.
- The process for granting door keys or access cards for IT facilities and resources shall include the approval of the person responsible for the facility or room.
- Access cards or keys issued for access to restricted IT facilities and resources may 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.
- Access records and sign-in logs shall be maintained and archived for routine review for a minimum of one year.
- No one shall be permitted to enter a controlled-access facility, area, or room without being authenticated and privileges verified.

Organizations responsible for IT facilities and resources shall designate a responsible party to review access records and visitor logs. These reviews shall be conducted at least every three months. The reviewer shall:

- Investigate any unusual access.
- Remove access privileges for individuals who no longer require right of entry.

Agencies shall ensure procedures are 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. Responsibilities

### 4.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

### 4.2 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 cooperate 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 to only 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 to be physically protected in proportion to the data or application's criticality or functional importance.

## 5. 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*
- *General Order 4.1, Security for Commonwealth Owned/Controlled Buildings, Property, Employees, and Visitor*

## 6. Authority

*Executive Order 2016-06, Enterprise Information Technology Governance*

## 7. 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.

## 8. 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<br>Added third-party vendors to Scope and Responsibilities<br>Added Related ITP Section<br>Added Exemption Section | N/A |
| Revision | 09/19/2022 | ITP Refresh<br>Added third party vendor requirements to Responsibilities section from OPD-SEC000B. | Revised IT Policy Redline <09/19/2022> |