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 are to take great care in physically securing IT facilities and resources to ensure the integrity of their systems and networks.

Physical access to other Commonwealth resources is regulated by the policies and procedures described in General Order No. 4.1: Security for Commonwealth Owned/Controlled Buildings, Property, Employees, and Visitors.

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 and hub rooms, voicemail system rooms, and similar areas containing IT facilities and resources.

All IT facilities and resources are to be physically protected in proportion to the criticality or functional importance.

Protection measures 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.

Access to restricted IT facilities and resources is limited only to authorized persons.

- The process for granting door keys or access cards for these facilities and resources shall include the approval of the person responsible for the facility or room.

- Access cards and/or keys issued for access to restricted IT facilities and resources may not be shared or loaned to others.

- Employees, business partners and citizen visitors without the proper access credentials 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/sign-out log. This log will have appropriate language on each page, or otherwise prominently displayed, indicating the minimal visitor responsibilities associated with accessing the facility.
  - 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 a party 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 period of not less than one year.

- No one shall be permitted to enter a controlled-access facility, area, or room without being authenticated and having his/her 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 is to:

- 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 comply with the requirements as outlined in this ITP.

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](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](http://www.oa.pa.gov/Policies/Pages/default.aspx)

6. **Authority**
   - Executive Order 2016-06, *Enterprise Information Technology Governance*

7. **Publication Version Control**
   It is the [Authorized User](http://www.oa.pa.gov/Policies/Pages/Glossary.aspx)’s responsibility to ensure they have the latest version of this publication, which appears on [https://itcentral.pa.gov](https://itcentral.pa.gov) for Commonwealth personnel and on the Office of Administration public portal: [http://www.oa.pa.gov/Policies/Pages/default.aspx](http://www.oa.pa.gov/Policies/Pages/default.aspx). Questions regarding this publication are to 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 is to be submitted via the enterprise IT policy waiver process. Refer to [ITP-BUS004 IT Policy Waiver Review Process](http://www.oa.pa.gov/Policies/Pages/default.aspx) for guidance.

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Purpose of Revision</th>
<th>Redline Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original</td>
<td>06/21/2007</td>
<td>Base Policy</td>
<td></td>
</tr>
<tr>
<td>Revision</td>
<td>04/02/2014</td>
<td>ITP Reformat</td>
<td></td>
</tr>
<tr>
<td>Revision</td>
<td>06/08/2021</td>
<td>• ITP Template</td>
<td>Revised IT Policy Redline &lt;06/08/2021&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added third-party vendors to Scope and Responsibilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Related ITP Section</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Exemption Section</td>
<td></td>
</tr>
</tbody>
</table>