pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Physical Security Policy for IT Resources

ITP Number	***Effective Date***
ITP-SEC029	June 21, 2007
Category	***Supersedes***
Recommended Policy	
Contact	***Scheduled Review***
RA-ITCentral@pa.gov	Annual

This Information Technology Policy (ITP) establishes policy for physical security of IT resources.

1. Purpose

Commonwealth agencies have physical access to Information Technology (IT) facilities and resources such as servers, tape libraries, and communication closets, which enables these agencies to bypass any application or operating system security. Agencies are to take great care in physically securing IT facilities and resources to ensure the integrity of their systems and networks.

The purpose of this policy is to establish an information security policy to ensure that commonwealth IT facilities and resources are protected by physical security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

Physical access to other commonwealth resources is regulated by the policies and procedures described in *Security for Commonwealth Owned/Controlled Buildings, Property, Employees, and Visitors.*

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

4. Policy

IT facilities and resources include data centers, computer rooms, telephone closets, network router 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 is to 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:

    - Are to 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.

    - Are to be issued a temporary identification badge and required to wear it openly.

    - Are to 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 are to be maintained and archived for routine review for a period of not less than one year.

- No one is to 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 are to designate a responsible party to review access records and visitor logs. These reviews are to 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 are to ensure procedures are in place to provide immediate access to IT facilities and resources to fire, safety, and other emergency personnel in the case of an emergency.

5. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

6. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision
Original	6/21/2007	Base Policy
	4/2/2014	ITP Reformat