COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF PUBLIC WELFARE

INFORMATION TECHNOLOGY POLICY

Name Of Policy: **Physical and Environmental Security Policy**	Number: **POL-SEC008**
Domain: **Security**	Category:
Date Issued: **06/09/11**	Issued By Direction Of:
Date Revised: **10/11/13**	 Sandra Patterson, CIO Bureau of Information Systems

Table of Contents

Document History

Version	Date	Author	Status	Notes
1.0	06/09/2011	David Johnson	Draft	Initial creation
2.0	06/23/2011	David Johnson	Draft	Revised per Tom Zarb review
2.1	10/11/2013	Pamela Skelton	Baseline	Revised per Pamela Skelton review

1 Introduction

1.1 Purpose

This policy establishes requirements for the implementation of physical and environmental safeguards to adequately protect Department of Public Welfare (DPW) personnel, property and information resources from unauthorized physical intrusion and other physical threats. This policy also addresses compliance with applicable DPW, Commonwealth of Pennsylvania (CoPA) and federal requirements.

1.2 Scope

All DPW employees, contractors and business partners are responsible for understanding and complying with this policy.

1.3 Compliance

All DPW employees, contractors and other stakeholders are expected to be familiar with and comply with this policy. Violations of this policy may lead to revocation of system privileges and/or disciplinary action. DPW employees who knowingly and willfully violate DPW, Commonwealth or federal law addressing improper use or disclosure of an individual's information may be subject to criminal investigation and prosecution or civil monetary penalties.

1.4 Exemptions

Requests for exemption to the policy should be submitted to the Chief Information Security Officer (CISO). Any exceptions granted will be issued a policy waiver for a defined period of time.

1.5 Policy Review and Update

This document, and its supporting standards and procedures, will be reviewed annually, and updated as needed.

2 Physical and Environmental Security Policy

Physical security represents the first line of defense against intruders and adversaries attempting to gain access to DPW facilities and/or information systems. Physical security restricts the entry and exit of personnel from protected areas, and protects sensitive data and systems. Environmental safety and security provides safeguards for fire safety, building environment, utilities, and other safeguards for the protection of DPW personnel, facilities and information resources.

DPW Policy

a. The physical security of DPW facilities, including facilities containing information resources, shall be managed per the following Commonwealth and DPW policies and standards:

- DPW Policy: Willow Oak Building Security.
- CoPA Policy: General Order 41, *Security for Commonwealth Owned/Controlled Buildings, Property, Employees and Visitors*
- CoPA Standards: *Minimum Standards for Improving Physical Security Access (*ITB-SEC029)

2.1 Physical Access

Physical Access is the enforcement of a set of rules that govern physical access authorizations at DPW. Effective physical access control is critical to verifying individual access authorizations before granting access to DPW facilities.

DPW Policy

a. DPW shall authorize physical access to the facility where the information system resides based on roles and responsibilities.
b. DPW shall require two (2) approved forms of identification before granting access to the facility where the information system resides.
c. The organization shall restrict unescorted access to the facility where the information system resides to personnel lacking sufficient security clearances and / or appropriate credentials.
d. Physical access authorizations shall be enforced to the information system in addition to physical access controls to DPW facilities.
e. Every physical access point to DPW facilities shall be equipped with at least alarms and/or guards where the information system resides, twenty-four (24) hours per day, seven (7) days per week.
f. DPW shall monitor physical intrusion alarms and surveillance equipment and employ centralized mechanisms to recognize the types of intrusions and initiate appropriate response actions.

2.2 Power Equipment and Cabling

Power equipment and cabling relate to the types of protection necessary to effectively protect equipment and cabling both internal and external to organizational facilities and environments of operation against damage and destruction.

DPW Policy

a. DPW shall employ power cable redundancy paths that are physically separated and automatic voltage controls for critical information system components.

2.3 Fire protection, Water damage protection and Temperature and humidity Controls

Fire protection, water damage protection and temperature and humidity controls represents the minimum requirements needed to protect DPW information system and its personnel against fire, water damage and temperature and humidity abnormal levels.

DPW Policy

Fire Protection

a. DPW Information system shall employ and maintain fire suppression and detection systems supported by an independent source of energy (e.g., handheld fire extinguishers, smoke detectors, sprinkler systems and fixed fire hose wheels)
b. In the event of a fire, those fire suppression and detection systems shall be activated automatically to notify the organization and proper emergency responders.
c. DPW shall employ automatic fire suppression capability when the facility is not staffed on a continuous basis.

Water Damage Protection

a. DPW shall employ automated centralized mechanisms to detect the presence of water in the information system and alerts the CISO.

Temperature and Humidity Controls

a. DPW shall define the acceptable temperature and humidity levels within the facility where the information system resides
b. The frequency to monitor temperatures and humidity levels shall be defined.
c. The organization shall then monitor the temperature and humidity with the organization-defined frequency

2.4 Emergency Shutoff / Power / Lighting

DPW information system has established appropriate controls in the event of a primary power source loss or power outage / disruption.

DPW Policy

Emergency Shutoff

a. In emergency situations, DPW shall provide the capability of shutting off power to either the information system or individual system components.

Emergency Power

a. In the event of a primary power source loss, DPW organization shall provide the following:
   - A short-term uninterruptible power supply to facilitate an eventual orderly shutdown of the information system.
   - A long-term self-contained, alternate power supply for the information system that is capable of maintaining minimally required operational capability

Emergency Lighting

a. In the event of a power outage or disruption, DPW Information system shall employ and maintain an automatic emergency lighting to cover emergency exits and evacuation routes within DPW facilities.

2.5 Monitoring Physical Access

DPW Policy

a. DPW shall review physical access logs every at least once every two (2) months.

3 Appendix

3.1 References

Document	Source
DPW Web Application Privacy Standard	DPW
Health Insurance Portability and Accountability Act (HIPAA) Privacy Implementation Handbook	DPW