COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT'S OF PUBLIC WELFARE, INSURANCE AND AGING

INFORMATION TECHNOLOGY POLICY

Name Of Policy: **Media Protection Policy**	Number: **POL-SEC006**
Domain: **Security**	Category:
Date Issued: **06/09/11**	Issued By Direction Of:  Sandra K. Patterson, CIO Bureau of Information Systems
Date Revised: **10/24/13**	

Table of Contents

1 Introduction

1.1 Purpose

This policy establishes requirements for the protection of DPW information that resides outside the protective boundaries of DPW information systems, on electronic or hard copy media. Requirements address labeling, access, backup, storage, sanitization, and disposal of information that resides on electronic and hard copy media. This policy also addresses compliance with applicable DPW, Commonwealth of Pennsylvania (CoPA) and federal requirements.

1.2 Scope

All DPW employees, contractors and other stakeholders are responsible for understanding and complying with this policy. This policy applies to all media capable of storing information, including electronic media (e.g., diskettes, magnetic tapes, USB drives, removable hard drives, compact discs, portable computing devices, printers, copiers), and hard copy media (e.g., paper, microfilm).

1.3 Compliance

Violations of this policy may lead to revocation of system privileges and/or disciplinary action.

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 Media Labeling

Media containing sensitive DPW information must be labeled, to communicate the required level of protection.

DPW Policy

a. Security control requirements for media containing DPW data shall be established. Requirements will address the levels of data sensitivity of media, as described in DPW's Data Classification Standard.

b. All media, including backup media and portable media, containing high sensitivity DPW information shall be clearly marked and labeled to indicate the classification(s) of the information it contains based on DPW's Data Classification Standard.

c. Removable magnetic media shall be uniquely labeled to be discernible from other media and receive security protections commensurate with the data therein.

3 Media Storage

Media containing sensitive DPW information must be securely stored, in accordance with the appropriate level of protection identified by DPW's Data Classification Standard.

DPW Policy

a. The security and integrity of DPW data stored on electronic media shall be protected from unauthorized access, intrusion, heat, magnetic fields and physical damage.

b. DPW employees and contractors shall only use Commonwealth approved portable devices on the DPW network.

c. Media used for high sensitivity DPW information system operation and restoration shall be physically protected and securely stored in a controlled area.

d. Data backups of operating system and other critical information system software shall be stored in secured fire-rated containers that are not collocated with the operational software.

e. DPW shall physically protect and securely store sensitive media at a level commensurate with the sensitivity of the data.

f. Data backups shall be secured in locked containers and transported for off-site storage on a periodic basis

g. Program Offices/System Owners and DPW users shall control access to, and securely store, all information system media (electronic and non-electronic) containing DPW sensitive information, including backup and removable media, in a secure location when not in use. Sensitive media shall be stored in locked canisters or encrypted if the information system media are removed from the primary storage area.

h. DPW users shall ensure that unattended laptops and other portable information systems are secured via a locking cable, locked office, or a locked cabinet.

4 Media Retention

Media records are to be kept available to support analysis relating to misuse, penetration reconstruction, or other investigations. The following policy provides guidance to ensure that media records are retained in accordance with DPW, CoPA and federal requirements, as well as to provide sufficient information to reconstruct the data in the event of a breach.

DPW Policy

a. DPW shall allocate sufficient media record storage capacity to reduce the likelihood of such capacity being exceeded.

b. The media records shall at a minimum, contain:

- Name of media recipient;
- Signature of media recipient;
- Date/time of media received;
- Media control number and contents;
- Movement or routing information; and
- If disposed of, the date, time, and method of destruction.

b. DPW media records shall be retained for at least 90 days to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention

DPW Policy

requirements.

5 Media Transport

Media containing sensitive DPW information must be protected during transport to prevent possible compromise.

DPW Policy

a. System owners shall document the movement of media and the person responsible for such movements.

b. DPW information systems external and internal interfaces shall be encrypted.

6 Media Access

Media containing sensitive DPW information must be accessible only by authorized individuals.

DPW Policy

a. DPW, business partners and vendors shall provide and maintain physical access controls for DPW media storage areas.

b. DPW, business partners and vendors shall maintain a record of the access of hardware and electronic media, and the person responsible for such access (DPW's HIPAA Security Handbook, Section 14.3, and Accountability).

c. DPW employees and contractors shall use only CoPA provided information systems disks, diskettes, portable storage devices or software to process, access, or store sensitive information.

d. System owners shall restrict access to DPW information systems to authorized individuals only.

7 Data Backup

Identified below are the requirements for the use of data backup media in providing for the reliable restoration of systems and files in the event of a disruption or disaster.

DPW Policy

a. Sensitive DPW data, operating system and related software, essential to the continued operation of critical DPW systems and services, shall be backed up.

b. Backup media must be protected in accordance with the highest DPW sensitivity level of information stored.

c. Backups shall be taken at periodic intervals, identified by the system owner or program office. Backup intervals shall be established to meet the time-criticality requirements of agency business processes, business continuity plans, and legal and regulatory requirements.

d. System owners shall establish, document and maintain data backup and recovery procedures.

e. Data backups shall be tested on a regular basis for restorability, recoverability, and to ensure that restored information has not been compromised.

f. Data backups shall be clearly and consistently labeled to facilitate restoration and testing, and to guard against mishandling, loss, or accidental overwriting.

g. DPW data on backup tapes shall be encrypted.

h. Physical access controls implemented at offsite backup storage locations shall meet the physical

DPW Policy

access controls of the source systems.

8 Electronic Media Sanitization and Disposal

Identified below are requirements for sanitization of data from media prior to disposal or reuse. Approved sanitization methods include crosscut shredding, degaussing, and use of approved disk-wiping software.

DPW Policy

a. Electronic and non-electronic media shall be sanitized prior to disposal or release for reuse. Media sanitization shall use CoPA approved processes, and comply with any applicable regulatory requirements, such as those defined in Internal Revenue Service Publication 1075 (IRS 1075) and the Health Information Portability and Accountability Act (HIPAA).

b. Processes for cleansing and disposal of computers, hard drives and fax/printer/scanner devices are provided in ITB-SYM009, *Commonwealth of Pennsylvania Data Cleansing Policy.*

c. Sanitization procedures shall be established and documented.

- Procedures shall include media sanitization, verification of sanitization, disposal, and reuse of media.
- Procedures shall specify the use of event logs.
- Procedures shall be periodically reviewed and updated as needed.

d. Media sanitization and disposal actions shall be tracked, documented, and verified. Documentation shall provide a record of the media sanitized, when, how media were sanitized, the person who performed the sanitization, and the final disposition of the media. The record of action taken should be maintained in a written or electronic format as defined by Security Audit Logging Policy.

e. DPW media sanitization equipment and procedures shall be tested at least annually to ensure correct performance.

e. Physical destruction shall be used for the disposal of digital media and data storage devices contained in equipment to be redeployed outside of DPW. Digital degaussing shall be the primary sanitization method for redeployment within DPW.

9 Hard Copy Media Disposal

Identified below are requirements for the destruction and disposal of hard copy media.

DPW Policy

a. Hard copy media containing DPW information shall by shredded, using a cross cut shredder, prior to disposal.

b. The Program Office shall monitor shredding and disposal of hard copy media, as required to ensure and verify compliance with policy.

10 Appendix

10.1 Supporting DPW Policies

Document	Type
Media Labeling	
Data Classification Standards	DPW Standard
Policy Regarding Portable Storage Devices and Removable Media	CoPA Memo
Media Access	
HIPAA Security Handbook (Section 6)	DPW Handbook
Use of Portable Storage Devices and Media	DPW Standard
Media Storage	
HIPAA Security Handbook (Sections 9, 14 and 15)	
Use of Portable Storage Devices and Media	DPW Standard
ITB-SEC019 - Policy and Procedures for Protecting Commonwealth Electronic Data	CoPA ITB
Media Sanitization	
HIPAA Security Handbook (Sections 14.1, 14.2)	DPW Handbook
Media Transport	
HIPAA Security Handbook (Section 14.3)	DPW Handbook
Data Backup	
Manual 210.8, Vital Records Disaster Planning	CoPA Manual
Data Encryption Standards DPW Standard	DPW Standard
Electronic Media Sanitization and Disposal	
HIPAA Security Handbook (Sections 14.1, 14.2)	DPW Handbook
ITB-SYM009 - Commonwealth of Pennsylvania Data Cleansing Policy	CoPA ITB

Policy Revision Log:

Change Date	Version	Change Description	Author and Organization
06/12/2011	1.0	Initial Creation	David Johnson
06/17/2011	2.0	Revised per Tom Zarb review	David Johnson
10/24/2013	2.1	Revised per Mathieu Saury review	Mathieu Saury