### Information Technology Policy

<table>
<thead>
<tr>
<th>Name Of Policy:</th>
<th>Media Protection Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number:</td>
<td>POL-SEC006</td>
</tr>
<tr>
<td>Domain:</td>
<td>Security</td>
</tr>
<tr>
<td>Date Issued:</td>
<td>06/09/11</td>
</tr>
<tr>
<td>Date Revised:</td>
<td>05/02/17</td>
</tr>
<tr>
<td>Issued By Direction Of:</td>
<td>Sandra K. Patterson, CIO Bureau of Information Systems</td>
</tr>
</tbody>
</table>
# Table of Contents

1 Introduction ............................................................................................................................ 3  
  1.1 Purpose ................................................................................................................................ 3  
  1.2 Scope .................................................................................................................................... 3  
  1.3 Compliance ....................................................................................................................... 3  
  1.4 Exemptions ......................................................................................................................... 3  
  1.5 Policy Review and Update ................................................................................................. 3  

2 Media Labeling ....................................................................................................................... 3  

3 Media Storage ........................................................................................................................ 4  

4 Media Retention ..................................................................................................................... 4  

5 Media Transport ..................................................................................................................... 5  

6 Media Access ........................................................................................................................ 5  

7 Data Backup ........................................................................................................................ 5  

8 Electronic Media Sanitization and Disposal ........................................................................... 6  

9 Hard Copy Media Disposal .................................................................................................... 7  

10 Appendix ................................................................................................................................ 8  
   10.1 Supporting DHS Policies ................................................................................................. 8
1 Introduction

1.1 Purpose
This policy establishes requirements for the protection of DHS information that resides outside the protective boundaries of DHS 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 DHS, Commonwealth of Pennsylvania (CoPA) and federal requirements.

1.2 Scope
All DHS 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 DHS information must be labeled, to communicate the required level of protection.

DHS Policy

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

b. All media, including backup media and portable media, containing high sensitivity DHS information shall be clearly marked and labeled to indicate the classification(s) of the information it contains based on DHS’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 DHS information must be securely stored, in accordance with the appropriate level of protection identified by DHS’s Data Classification Standard.

**DHS Policy**

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

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

c. Media used for high sensitivity DHS 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. DHS 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 DHS users shall control access to, and securely store, all information system media (electronic and non-electronic) containing DHS 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. DHS 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 DHS, CoPA and federal requirements, as well as to provide sufficient information to reconstruct the data in the event of a breach.

**DHS Policy**

a. DHS 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. DHS 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
5 Media Transport

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

DHS Policy

- System owners shall document the movement of media and the person responsible for such movements.
- DHS information systems external and internal interfaces shall be encrypted.

6 Media Access

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

DHS Policy

- DHS, business partners and vendors shall provide and maintain physical access controls for DHS media storage areas.
- DHS, business partners and vendors shall maintain a record of the access of hardware and electronic media, and the person responsible for such access (DHS’s HIPAA Security Handbook, Section 14.3, and Accountability).
- DHS employees and contractors shall use only CoPA provided information systems disks, diskettes, portable storage devices or software to process, access, or store sensitive information.
- System owners shall restrict access to DHS 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.

DHS Policy

- Sensitive DHS data, operating system and related software, essential to the continued operation of critical DHS systems and services, shall be backed up.
- Backup media must be protected in accordance with the highest DHS sensitivity level of information stored.
- 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.
- System owners shall establish, document and maintain data backup and recovery procedures.
- Data backups shall be tested on a regular basis for restorability, recoverability, and to ensure that restored information has not been compromised.
- Data backups shall be clearly and consistently labeled to facilitate restoration and testing, and to guard against mishandling, loss, or accidental overwriting.
DHS Policy

g. DHS data on backup tapes shall be encrypted.

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

i. The eCIS and COMPASS web application data and hosting servers are stored in the Commonwealth datacenter located at Harrisburg, PA.

DHS leverages CommVault for taking disk based back-ups. The National Institute of Standards and Technology has CommVault’s certification under the list of Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules that have been tested using the cryptographic module validation program (CMVP). The data will be backed up in HDC.

(HDC is Harrisburg Data Center)

BIS Database Management Section performs a daily backup of the eCIS web application in addition a daily incremental backup using CommVault solution, and data is transferred on to in Harrisburg Data Center. The backups are maintained for 30 days. All backups are disk based. There are no tape based backups.

The new commonwealth datacenter at Ashburn, VA does not have a tape based back-up process. All the back-ups are disk-based backs using Commvault. There is not data in physical form entering or exiting the facility.

j. Media Protection Procedures: BIS Security Architecture Section and the Commonwealth datacenter are responsible to establish appropriate procedures to protect data at rest (media). Commonwealth datacenter uses the existing Media Protection procedures/mechanisms that are designed to address the IRS Publication 1075 requirements.

DHS leverages CommVault for taking disk based back-ups. The National Institute of Standards and Technology has CommVault's certification under the list of Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules that have been tested using the cryptographic module validation program (CMVP). The data will be backed up in HDC. (HDC is Harrisburg Data Center)

BIS Database Management Section performs a daily backup of the eCIS web application in addition a daily incremental backup using CommVault solution, and data is transferred on to in Harrisburg Data Center. The backup are maintained for 30 days. All backups are disk based. There are no tape based backups.

The new commonwealth datacenter at Ashburn, VA does not have a tape based back-up process. All the back-ups are disk-based backs using Commvault. There is not data in physical form entering or exiting the facility.

BIS Security Architecture Section has established the annual information security risk self-assessment program that covers the physical and environmental safeguards of the DHS facility and the Commonwealth datacenter. The process is described in section RA-3.

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.

DHS 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. DHS 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 DHS. Digital degaussing shall be the primary sanitization method for redeployment within DHS.

9 Hard Copy Media Disposal

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

DHS Policy

a. Hard copy media containing DHS 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 DHS Policies

<table>
<thead>
<tr>
<th>Document</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Media Labeling</strong></td>
<td></td>
</tr>
<tr>
<td>Data Classification Standards</td>
<td>DHS Standard</td>
</tr>
<tr>
<td>Policy Regarding Portable Storage Devices and Removable Media</td>
<td>CoPA Memo</td>
</tr>
<tr>
<td><strong>Media Access</strong></td>
<td></td>
</tr>
<tr>
<td>HIPAA Security Handbook (Section 6)</td>
<td>DHS Handbook</td>
</tr>
<tr>
<td>Use of Portable Storage Devices and Media</td>
<td>DHS Standard</td>
</tr>
<tr>
<td><strong>Media Storage</strong></td>
<td></td>
</tr>
<tr>
<td>HIPAA Security Handbook (Sections 9, 14 and 15)</td>
<td></td>
</tr>
<tr>
<td>Use of Portable Storage Devices and Media</td>
<td>DHS Standard</td>
</tr>
<tr>
<td>ITB-SEC019 - Policy and Procedures for Protecting Commonwealth Electronic Data</td>
<td>CoPA ITB</td>
</tr>
<tr>
<td><strong>Media Sanitization</strong></td>
<td></td>
</tr>
<tr>
<td>HIPAA Security Handbook (Sections 14.1, 14.2)</td>
<td>DHS Handbook</td>
</tr>
<tr>
<td><strong>Media Transport</strong></td>
<td></td>
</tr>
<tr>
<td>HIPAA Security Handbook (Section 14.3)</td>
<td>DHS Handbook</td>
</tr>
<tr>
<td><strong>Data Backup</strong></td>
<td></td>
</tr>
<tr>
<td>Data Encryption Standards DHS Standard</td>
<td>DHS Standard</td>
</tr>
<tr>
<td><strong>Electronic Media Sanitization and Disposal</strong></td>
<td></td>
</tr>
<tr>
<td>HIPAA Security Handbook (Sections 14.1, 14.2)</td>
<td>DHS Handbook</td>
</tr>
<tr>
<td>ITB-SYM009 - Commonwealth of Pennsylvania Data Cleansing Policy</td>
<td>CoPA ITB</td>
</tr>
</tbody>
</table>
Policy Revision Log:

<table>
<thead>
<tr>
<th>Change Date</th>
<th>Version</th>
<th>Change Description</th>
<th>Author and Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/12/2011</td>
<td>1.0</td>
<td>Initial Creation</td>
<td>David Johnson</td>
</tr>
<tr>
<td>06/17/2011</td>
<td>2.0</td>
<td>Revised per Tom Zarb review</td>
<td>David Johnson</td>
</tr>
<tr>
<td>10/24/2013</td>
<td>2.1</td>
<td>Revised per Mathieu Saury review</td>
<td>Mathieu Saury</td>
</tr>
<tr>
<td>05/02/2017</td>
<td>2.2</td>
<td>Annual Updation</td>
<td>John Miknich</td>
</tr>
</tbody>
</table>