COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF HUMAN SERVICES, INSURANCE AND AGING

INFORMATION TECHNOLOGY POLICY

Name Of Policy: **Cryptography Policy**	Number: **POL-SEC002**
Domain: **Security**	Category:
Date Issued: **06/09/11**	Issued By Direction Of: 
Date Revised: **05/05/2017**	Sandra K. Patterson, CIO Bureau of Information Systems

Table of Contents

1 Introduction

1.1 Purpose

This policy establishes requirements for the use of cryptography to protect DHS information resources that contain, process, or transmit confidential and DHS-sensitive information. Additionally, this policy provides direction to ensure that Commonwealth of Pennsylvania (CoPA) and federal requirements are followed.

1.2 Background

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process. DHS information systems must use appropriate cryptographic controls to ensure the protection of data and communications. Uses of cryptography for DHS information systems include:

- Encrypt data while in storage (e.g., hard drives, diskettes, and tapes).
- Encrypt data while in transmission.
- Encrypt individual files for transmission over an unsecured medium.
- Encrypt email messages.
- Guarantee the integrity of a file or message, and detect any modifications.
- Provide the legally binding, digital equivalent of a written signature.
- Support non-repudiation.
- Support authentication.

1.3 Scope

All DHS employees, contractors and business partners are responsible for understanding and complying with this policy. This policy addresses encryption policy and controls for confidential and other DHS-sensitive data that is at rest (including portable devices and removable media), data in motion (transmission security), and encryption key standards and management.

1.4 Compliance

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

1.5 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.

1.6 Policy Review and Update

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

2 General Encryption Policy

Identified below are requirements for the use of cryptography to protect sensitive DHS information. Sensitivity of data is based on privacy concerns, statutory or regulatory obligations for data handling, or risk of financial loss to the Commonwealth or its clients, business associates, or citizens.

DHS Policy

a. DHS information shall be protected using approved data encryption techniques, including:
   - DHS information stored on desktops, portable computing devices (e.g., laptops, PDAs), portable storage media (e.g., CDs, DVDs, USB flash drives, backup tapes, removable hard drives) and databases. Guidance for the encryption of data at rest is provided in ITB-SEC020, *Encryption Standards for Data at Rest* and DHS's *Data Encryption Standards*.
   - DHS information transmitted over a public network. Additional guidance for the encryption of data in transit is provided in ITB-SEC031, *Encryption Standards for Data in Transit* and DHS's *Data Encryption Standards.*
   - Emails to business partners containing DHS information shall be sent using Commonwealth's secure email service in accordance with ITB-SEC008, Enterprise E-mail Encryption

b. A key recovery/regeneration mechanism shall be implemented so that encrypted information can be decrypted and accessed by authorized personnel. Use of encryption keys which are not recoverable by authorized personnel is prohibited.

c. Business partners and DHS vendors who store or transmit DHS information shall comply with this policy.

d. DHS information systems that use electronic signatures shall meet the requirements specified by the *Commonwealth of Pennsylvania Electronic Signature Policy (ITB-SEC006)*.

3 Appendix

3.1 References

Document	Type
Data Encryption Standards	DHS policy
E-Signature Bill (P.L. 071 #69)	CoPA Law
HIPAA Security Handbook (Section 14.3)	DHS Handbook
HIPAA: Security and Electronic Signature Standard; Proposed Rule (DHHS 45 CFR 142)	DHHS Rule
HIPAA: Standards for Electronic Transactions; Announcement of Designated Standard Maintenance Organizations; Final Rule and Notice (DHHS 45 CFR 160 and 162)	DHHS Rule
ITB-B.5. - Security & Digital Certificate Policy and Encryption & Internet/Intranet Browser Standards for e-Government Web Sites & Applications	CoPA ITB
ITB-SEC006 - Commonwealth of Pennsylvania Electronic Signature Policy	CoPA ITB
ITB-SEC020 - Encryption Standards for Data at Rest	CoPA ITB
ITB-SEC031 - Encryption Standards for Data in Transit	CoPA ITB
MD 210.12 - Electronic Commerce Initiatives and Security	CoPA MD
GEN-SEC013G, Enterprise Public Key Infrastructure	CoPA Standard

Document	Type
STD-SEC014C, *Product Standards for Public Key Infrastructure/Shared Service Provider*	CoPA Standard

Policy Revision Log:

Change Date	Version	Change Description	Author and Organization
06/09/2011	1.0	Initial creation	David Johnson
06/17/2011	2.0	Revised per T. Zarb review	David Johnson
10/24/2013	2.1	Revised per M. Saury review	Mathieu Saury
05/05/2017	2.2	Annual Revision	John Miknich