pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Encryption Standards for Data at Rest

ITP Number	***Effective Date***
ITP-SEC020	August 17, 2007
Category	***Supersedes***
Recommended Policy	
Contact	***Scheduled Review***
RA-ITCentral@pa.gov	Annual

This Information Technology Policy (ITP) establishes policy and standards for encryption for data at rest.

1. Purpose

The purpose of this Information Technology Policy (ITP) is to improve the confidentiality and integrity of data at rest by requiring the use of encryption.

2. Background

"Data at rest" refers to all data in storage, regardless of the storage device, that is not in motion. This excludes information traversing a network or temporarily residing in non- volatile computer memory. Data at rest primarily resides in files on a file system. However, data at rest is not limited to file data. Databases, for example, are often backed by data files, and their contents can be thought of as rows and columns of data elements instead of as individual files. Agencies should consider all aspects of storage when designing an encryption solution.

Criteria to be taken into account when encrypting data at rest include:

- Data Classification – Refer to ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data,* to determine the classification of sensitive, protected, and exempt data.
- Statutory or regulatory mandates including, but not limited to, the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act of 2002, the Gramm- Leach-Bliley Act (GLBA), and any other law or regulation involving data security at rest.

Data encryption supports data privacy and integrity by providing a method to convert electronic information into a format that is readable only by authorized individuals. This policy establishes the use of the following types of encryption for electronic information:

- **Full Disk Encryption**: Full disk encryption is a computer security technique that encrypts data stored on a mass storage or removable device, and automatically decrypts the information when an authorized user requests it. Full disk encryption is often used to signify that everything on a disk or removable device, including the operating system and other executables, is encrypted. Full disk encryption includes hardware encryption, such as configuring a tape drive to encrypt all backup data before write.

- **File Encryption**: File encryption is a technique that encrypts files on a file system, without encrypting the file system itself or the entire disk. A file encrypting application may include functionality to: archive multiple files into a single file before or after encrypting; produce self-decrypting files; or automatically encrypt files or folders based on policies or locations. File encryption is often used to protect files being sent through email or written to removable media.

- **Data Element Encryption**: Data element encryption is a technique that encrypts individual data elements instead of encrypting an entire file or database. Common examples of data element encryption include column level database encryption and encryption of a Social Security Number (SSN) before writing it to a file. Data element encryption is used to selectively apply encryption, and may be used to reduce encryption/decryption overhead, to protect different elements with different keys, or to simplify adding encryption to applications.

3. 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

Agencies must protect stored sensitive, protected, or exempt data at rest through the use of encryption. Additionally, agencies must ensure that any non-commonwealth entity or agency business partner/contractor which stores or has access to such data also protects stored sensitive, protected, or exempt data at rest through the use of encryption. Agencies are to adhere to the Advanced Encryption Standard (AES) for symmetric encryption. For asymmetric encryption, agencies are to follow ITP-SEC013 - *Identity Protection and Access Management (IPAM) Architectural Standard - Identity Management Services*, and ITP- SEC014 - *IPAM Architectural Standard – Identity Management Technology Standards*.

Full Disk Encryption:

Full disk encryption conforming to AES specifications is to be used on laptop computers, other mobile computing devices, and electronic devices for which physical security controls are limited due to the mobile nature of the devices. In cases where these devices will not store any sensitive, protected, or exempt data, exceptions may be granted. Agencies are to comply with product

standards as described in section 5 of this ITP for these devices.

Full disk encryption is also to be used on computers or computing devices storing sensitive, protected, or exempt data located in areas not equipped with public access restrictions and physical security controls such as locked doors etc. Agencies are to comply with product standards as described in section 5 of this ITP for these devices as well.

In order to ensure the highest levels of security and overall effectiveness of disk encryption, devices using full disk encryption are not to be placed in suspend mode when unattended, and are to be shut down completely when not in use or when unattended.

Full disk encryption is to be used for archiving or backing up sensitive, protected, or exempt data to tape or optical media. Software or hardware mechanisms can be used provided they conform to AES specifications. If no conforming mechanisms are available, file encryption techniques may be used to encrypt the data at the file level before it is written to tape or optical media.

File Encryption:
File encryption is to be used when files containing sensitive, protected, or exempt data are transferred on physical media, through email, or across networks, without other forms of encryption or protection.

Data Element Encryption:
Data element encryption is to be used when sensitive, protected, or exempt data elements are stored. Physical security of a data storage device is not a substitute for data element encryption, as it does not prevent accessing data through exploited application vulnerabilities. Likewise, data element encryption should be designed such that exploited access does not provide unencrypted access to sensitive, protected, or exempt data.

5. Encryption Product Standards for Data at Rest

CURRENT STANDARDS

(These technologies meet the requirements of the current architecture and are recommended for use.)

Technology	Platforms	Technology Classification
Full Disk Encryption McAfee Endpoint Encryption	Microsoft Windows XP Microsoft Windows 2003 Microsoft Vista Windows 7	Current
Full Disk Encryption BitLocker Drive Encryption Encryption	Windows 7 Enterprise (requires Microsoft Software Assurance package)	Current
Content Encryption McAfee Endpoint Content	Microsoft Windows XP Microsoft Windows 2003	Current

Encryption (formerly SafeBoot Content Encryption)	Microsoft Vista Windows 7	
Content Transport Encryption Rijndael - 256 bit e.g., devices/software: Advanced Encryption Standard (AES) algorithm; SafeBoot USB Phantom; UltraLock USB; Kingston DataTraveler; dm-crypt	Microsoft Windows XP Microsoft Windows 2003 Microsoft Vista Windows 7 Linux Mac	Current

Note: Content Encryption/Content Transport Encryption are not for use on non-removable media.

CONTAIN

(These technologies no longer meet the requirements of the current architecture and are not recommended for use. They are to be phased out over time. No date has been set for their discontinuance.)

Technology	Platforms	Technology Classification
--	--	Contain

RETIRE

(These technologies are being phased out. Plans are to be developed for their replacement, especially if there is risk involved, such as lack of vendor support. A date for retirement has been set.)

Technology	Platforms	Technology Classification
SafeBoot Device Encryption	Microsoft Windows XP Microsoft Windows 2003 Microsoft Vista Windows 7	12/31/2013
SafeBoot Content Encryption	Microsoft Windows XP Microsoft Windows 2003 Microsoft Vista Windows 7	12/31/2013
TrueCrypt Whole Disk	Microsoft Windows XP Microsoft Windows 2003 Microsoft Vista Windows 7 Linux Mac	06/20/2014
TrueCrypt in AES-256	Microsoft Windows XP Microsoft Windows 2003 Microsoft Vista Windows 7	06/20/2014

	Linux Mac	

EMERGING / RESEARCH

(Emerging technologies have the potential to become current standards. At the present time, they are to be used only in pilot or test environments where they can be evaluated. Use of these technologies is restricted to a limited production mode, and requires approval of a waiver request. Research technologies are less widely accepted and time will determine if they will become a standard.)

Technology	Platforms	Technology Classification
--	--	Emerging / Research

6. Responsibilities

Agencies are required to perform the actions outlined in this policy.

7. Related ITPs/Other References

- ITP-SEC013 - *Identity Protection and Access Management (IPAM) Architectural Standard - Identity Management Services*
- ITP-SEC014 - *IPAM Architectural Standard – Identity Management Technology Standards*
- ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*

8. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

9. 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	8/17/2007	Base Policy
Revision	10/16/2008	Updated to meet newly identified needs for encryption of data at rest
Revision	9/17/2009	Tape media update
Revision	1/21/2011	Updated to provide requirements and guidance on encryption data at rest without specificity to disks and removable media
	4/2/2014	ITP Reformat; Merged STD-SEC020A into ITP
Revision	6/20/2014	Moved "TrueCrypt in AES-256" & "TrueCrypt Whole Disk" to Retire Standards table due to security risk