pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Encryption Standards for Data at Rest

ITP Number ITP-SEC020	**Effective Date** August 17, 2007
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** October 2020

1. Purpose

To improve the confidentiality and integrity of data at rest by requiring the use of encryption.

2. 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.

3. 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 considered 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

4. Definitions

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 can include hardware encryption and self-encrypting, such as configuring a tape drive to encrypt all backup data before write. Storage area network (SAN) device encryption can be met with data-at-rest encryption with self-encrypting drives.

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 selfdecrypting 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.

5. Policy

Agencies must protect stored sensitive, protected, or exempt data at rest using encryption. Refer to ITP-SEC031 *Encryption Standards for Data in Transit* for current list of acceptable encryption standards*.* 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 using encryption.

Full Disk Encryption

Full disk encryption conforming to AES specifications is to be used on laptop computers, other mobile computing devices, portable storage 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 OPD-SEC020A *Encryption Product Standards for Data at Rest* 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. Agencies are to comply with product standards as described in OPD-SEC020A *Encryption Product Standards for Data at Rest* for these devices.

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.

Non-encrypted flash drives may be procured from the Peripheral contract(s) only in cases where these devices will not store any sensitive, protected, or exempt data, as defined in ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data* or if the agency has capability to fully encrypt portable storage devices to standards as described in OPD-SEC020A *Encryption Product Standards for Data at Rest,* exceptions are granted without a waiver.

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.

6. Responsibilities

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

7. Related ITPs/Other References

Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal:
http://www.oa.pa.gov/Policies/Pages/default.aspx

- Management Directive 205.34 *Commonwealth of PA Information Technology Acceptable Use Policy*
- OPD-SEC020A - *Encryption Product Standards for Data at Rest* (Authorized COPA Personnel only. Contact RA-ITCentral@pa.gov for information)
- ITP-PRV001 - *Commonwealth of Pennsylvania Electronic Information Privacy Policy*
- ITP-SEC000 – *Information Security Policy*
- ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*

8. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

9. Exemption from This Policy

In the event an agency chooses to seek an exemption from the guidance within this IT policy, a request for a policy waiver is to be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT Waiver Review Process* for guidance.

10. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline
Original	08/17/2007	Base Policy	N/A
Revision	10/16/2008	Updated to meet newly identified needs for encryption of data at rest	N/A
Revision	09/17/2009	Tape media update	N/A
Revision	01/21/2011	Updated to provide requirements and guidance on encryption data at rest without specificity to disks and removable media	N/A
Revision	04/02/2014	ITP Reformat; Merged STD-SEC020A into ITP	N/A

Revision	06/20/2014	Moved “TrueCrypt in AES-256” & “TrueCrypt Whole Disk” to Retire Standards table due to security risk	N/A
Revision	01/02/2018	Moved Product Standards to OPD-SEC020A Added Exemption section Removed references to ITP-SEC013 and ITP-SEC014 Added full-disk encryption requirement for portable storage devices	N/A
Revision	10/15/2019	Added guidance for flash drives	Revised IT Policy Redline <10/15/2019>