pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Encryption Standards

ITP Number ITP-SEC031	**Effective Date** August 17, 2007
Category Security	**Supersedes** --
Contact RA-ITCentral@pa.gov	**Scheduled Review** June 2022

1. Purpose

This Information Technology Policy (ITP) establishes standards for the encryption of Commonwealth data while in transit and at rest.

2. Scope

This ITP applies to all departments, offices, boards, commissions, and councils under the Governor's jurisdiction (hereinafter referred to as "agencies"). Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP that are applicable to the products and services provided to the Commonwealth.

3. Definitions

3.1 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.

3.2 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 request it. The term "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.

3.3 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.

3.4 Volume Level Encryption: Protects a smaller subset of the drive, possibly down to

the individual folders. This can span a single disk or multiple disks.

4. Policy

4.1 Data in Transit

Encryption shall be used to protect the transmission of Class "C" Classified Records or Closed Records as defined in ITP-SEC019 *Policies and Procedures for Protecting Commonwealth Electronic Data*. Data in transit is any type of information that is actively moving between systems, applications, or locations. Encryption of data in transit is an effective data protection measure to protect data that is in motion.
Criteria to be taken into account when encrypting data in transit include:

- Data Classification - Refer to ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*, to correctly identify the categorization and classification of Commonwealth data.

- Data Compliance - Mandates of law 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 that involves data that is subject to some degree of protection under such statute, law, order, or regulation.

The Commonwealth Metropolitan Area Network (MAN) should not be considered a trusted mode of transit (i.e., zero trust network) and all data traffic through the MAN and Commonwealth agency networks should be considered untrusted unless additional interagency traffic encrypted trusts are established and maintained. Agencies must comply with all Security IT policy guidance to properly secure all Commonwealth data in transit.

Use of Advanced Encryption Standard (AES) for symmetric encryption is required.

Internet Protocol Security (IPSec) gateway to gateway implementations utilizing triple data encryption standard (3DES) is to be migrated to IPSec/AES to take advantage of increased security; new IPSec implementations are not to use 3DES.

Any application protocols (e.g., HTTP, file transfer protocol [ftp], secure copy [SCP]) tunneled in an encryption mechanism or combination of encryption mechanisms utilizing approved symmetric or asymmetric encryption algorithms as detailed in this policy are considered to be secure.

Use of 256-bit key sizes and hashing algorithms that utilize 160-bit (or greater) digest lengths are strongly recommended. Agencies are encouraged to use larger key/digest sizes where performance and client constraints allow.

Encryption products used to protect sensitive information are to conform to the NIST Cryptographic Module Validation Program listing http://csrc.nist.gov/groups/STM/cmvp/.

Transmission Mechanism Examples	Meets ITP-SEC031 for Internet communications, establishment of VPN tunnels for secure connections, remote administration technologies and VDI/Appstreaming uses
HTTPS in export grade ciphers (40-bit and 56-bit keys)	No, does not meet key size requirements, and does not utilize AES.
HTTPS protocols (any SSL version, TLS 1.0 (not permitted), TLS 1.1) Ciphers including Rivest 4 (RC4) and 3DES ciphers	No
HTTPS protocols 1.2 , 1.3 (emerging) Ciphers shall be AES 128 bit or higher. ECDHE is also approved for use. TLS 1.3 is an emerging technology. When vendors provide TLS 1.3 capable server software, appropriate testing will need to be performed to ensure application compatibility.	Yes
Secure Shell (SSH)-1, SSH-2 (3DES, or Blowfish)	No, does not utilize AES encryption.
SSH-2 (AES), SCP/SFTP over SSH-2, HTTP over SSH-	Yes
VPN Clients 1.2 , 1.3 (emerging) passwords or PKI certificates). TLS 1.3 is an emerging technology. When vendors provide TLS 1.3 capable server software, appropriate testing will need to be performed to ensure application compatibility.	Yes
IPSec (3DES for encryption)	No, IPSec/3DES setups are to be migrated to IPSec/AES.
IPSec (AES-CBC for encryption)	Yes
Layer 2 Forwarding (L2F) or Point-to-Point Tunneling Protocol (PPTP)	No, L2F and PPTP do not offer encryption.
SHA-1 cipher for certificate signing	Contain.
SHA-2 family of ciphers for certificate signing (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256)	Yes
SHA-3 family of ciphers for certificate signing (SHA3-224, SHA3-256, SHA3-384, SHA3-512; XOFs: SHAKE128, SHAKE256)	Yes

4.2 Data at Rest

Encryption shall be used to protect Class “C” Classified Records or Closed Records at rest. Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Encryption of data at rest is an effective data protection measure to protect inactive data.

To ensure the highest level of security and overall effectiveness of encryption, mobile or portable devices using encryption shall not be placed in suspend mode when unattended and shall be shut down completely when not in use or when unattended.

Full Disk Encryption

Full Disk Encryption shall be used on computers or computing devices storing Class “C” Classified Records or Closed Records located in areas not equipped with public access restrictions and physical security controls such as locked doors.

Full Disk Encryption shall be used for archiving or backing up Class "C" Classified Records or Closed Records to tape or optical media. Software or hardware mechanisms can be used provided they conform to Commonwealth standards. 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 Class "C" Classified Records or Closed Records as defined in ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data*.

Volume Level Encryption

In cases where the volume contains Class "C" Classified Records or Closed Records that are not encrypted by some other means of File or Data Element Encryption, Volume Level Encryption shall be used.

All volumes on mobile or portable device shall use at least Volume Level Encryption.

File Encryption

File Encryption shall be used when files containing Class "C" Classified Records or Closed Records are transferred on physical media, through email, or across networks, without other forms of encryption or protection.

Data Element Encryption

Data Element Encryption shall be used when Class "C" Classified Records or Closed Records are stored in accordance with ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data*. 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 Class "C" Classified Records or Closed Records.

5. Responsibilities

5.1 Agencies shall comply with the requirements as outlined in this ITP.

5.2 Office of Administration, Office of Information Technology shall comply with the requirements as outlined in this ITP.

5.3 Third-party vendors, licensors, contractors, or suppliers shall comply with the requirements as outlined in this ITP.

6. Related ITPs/Other References

Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx

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 Amended *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- ITP-PRV001 – *Commonwealth of Pennsylvania Electronic Information Privacy Policy*
- ITP-SEC000 – *Information Security Policy*
- ITP-SEC019 – *Policy and Procedures for Protecting Commonwealth Electronic Data*
- ITP-SFT005 - *Managed File Transfer (MFT)*

7. Authority

Executive Order 2016-06, *Enterprise Information Technology Governance*

8. Publication Version Control

It is the Authorized 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.

9. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, 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.

This chart contains a history of this publication's revisions:

Version	Date	Purpose of Revision	
Original	08/17/2009	Base Policy	
Revision	09/17/2009	Rewrote policy section and added transmission mechanism table	
Revision	04/02/2014	ITP Reformat	
Revision	08/17/2015	Revised Data sensitivity classification categories language regarding SEC019	
Revision	12/09/2016	• Revised Transmission Mechanism Examples table with updated encryption protocol requirements • Added Exemption section • Added ITP-SEC000 reference • Revised NIST Cryptographic Module Validation Program URL • Added Secure Hash Algorithm (SHA) language	
Revision	10/24/2017	• Added statement on "untrusted network" of Commonwealth MAN and agency networks in Policy section • Added additional References • Moved language from Purpose to Policy section for clarity	
Revision	07/22/2018	• Added TLS 1.1 to Contain, 1.2 and 1.3 are preferred • SSL/TLS 1.0 and lower no longer acceptable encryption protocol • Revised table for clarity	
Revision	12/04/2020	• Combined ITP-SEC020 Encryption Standard for Data at Rest with ITP-SEC031. SEC020 was added to this policy as Section 4.2 under Policy. • Added Definition section	Revised IT Policy Redline <12/4/2020>
Revision	06/22/2021	• Added disclaimer regarding TLS 1.3 • Updated Scope • Updated Related ITPs Section • Updated Transmission Mechanism Table Header • Language cleaned up throughout policy to be inclusive of third party vendors	Revised IT Policy Redline <06/22/2021>