pmrs pennsylvania
MUNICIPAL RETIREMENT SYSTEM

Board Information Technology Policy
Encryption Standards

Board Policy
2023-01

Effective Date March 16, 2023

Scheduled Review - Annually

Category
Security
Any reference to the Commonwealth in this policy includes the Pennsylvania Municipal Retirement Board, the Pennsylvania Municipal Retirement System (PMRS) and PMRS' contractors and consultants

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 offices, departments, 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. Policy

3.1 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 – Legal requirements such as, 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 protection by statute 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. Use of Elliptic Curve Diffie-Hellman encryption (ECDHE), Digital Signature Algorithm (DSA), or Rivest-Shamir-Adelman (RSA) for asymmetric encryption is required.

Internet Protocol Security (IPSec) gateway to gateway implementations utilizing triple data encryption standard (3DES) shall be migrated to IPSec/AES to take advantage of increased security; 3DES is prohibited for new IPSec implementations.

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 shall conform to the NIST Cryptographic Module Validation Program listing.

3.2 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.

4. Responsibilities

A. Agencies shall comply with the requirements as outlined in this ITP and the product standards in STD-SEC031A, *Encryption Configurations and Product Standards for Commonwealth Data (*Commonwealth Authorized Access Only*)*.

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

C. Third-party vendors, licensors, contractors, or suppliers shall:

- Ensure protection of Commonwealth data that is stored within contractor systems.
- Ensure Commonwealth Class "C" Classified Records or Closed Records are encrypted during transit and rest per ITP-SEC031, ITP-SEC019 and the NIST Cryptographic Module Validation Program.
- Ensure use of full disk encryption for archiving and backup of Class "C" Classified Records or Closed Records.
- Ensure non-Windows environments requiring full disk encryption, use full disk encryption that conforms to this ITP, AES specifications, and the NIST Cryptographic Module Validation Program.
- Ensure use of data element encryption when Class "C" Classified Records or Closed Records data elements are stored within a database. Transparent Data Encryption (TDE) or other database specific methods can be utilized to meet this requirement.

- Ensure for systems or data containing Criminal Justice Information, Criminal Justice Information Services (CJIS) Policy requirements are met.
- Ensure for systems receiving, processing, or storing Federal Tax Information (FTI), IRS Publication 1075 requirements must be met.

5. 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*
- STD-SEC031A, *Encryption Configurations and Product Standards for Commonwealth Data*
- 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)*
- NIST Cryptographic Module Validation Program
- NIST 800-77 Rev 1 Guide to IPSec VPNs
- CJIS Security Policy
- IRS Publication 1075

6. Authority

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

7. 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 shall be directed to RA-ITCentral@pa.gov.

8. 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 shall be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004, *IT Policy Waiver Review Process* for guidance.

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 Link
Original	08/17/2009	Base Policy	N/A
Revision	09/17/2009	Rewrote policy section and added transmission mechanism table	N/A
Revision	04/02/2014	ITP Reformat	N/A
Revision	08/17/2015	Revised Data sensitivity classification categories language regarding SEC019	N/A
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	N/A
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	N/A
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	N/A
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	N/A
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	N/A
Revision	08/18/22	ITP Refresh Replaced definitions with links to glossary Added policy language for asymmetrical encryption. Added third party vendor requirements under Responsibilities section from OPD-SEC000B. Updated Reference section and links. Removed table from Data in Transit section and moved to STD-SEC031A. Links not maintained by Commonwealth updated to homepages rather than direct links per Legal Direction.	Revised IT Policy Redline <08/18/2022>

Adopted by the Pennsylvania Municipal Retirement Board, March 16, 2023

Barry L Sherman

Barry Sherman, Chair