# Encryption Policy

| | |
|---|---|
| **Effective Date:**<br>January 06, 2025 | **Category:**<br>Security |
| **Scheduled Review:**<br>June 30, 2025 | **Supersedes:**<br>ITP-SEC031, ITP-SEC008 |

## 1. Authority

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

## 2. Purpose

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

## 3. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this policy as outlined herein.

## 4. Policy

For definitions found within this document, refer to the *IT Policy Glossary*.

### 4.1 Data in Transit

Encryption of Data In Transit is an effective data protection measure to protect data that is in motion. Encryption shall be used to protect the transmission of Class "C" Classified Records or Closed Records as defined in the *Data Classification Policy.*

The following criteria should be considered when encrypting Data In Transit:

- Data Classification - Refer to *Data Classification Policy,* to correctly identify the categorization and classification of Commonwealth data. Agencies shall ensure Personally Identifiable Information (PII) has been properly identified and classified and is encrypted during transit in accordance with all applicable laws and Commonwealth policies.
- 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 encryption is established and maintained. Agencies shall comply with all 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 STD-SEC031A, Encryption Configurations and Product Standards for Commonwealth Data are permitted.

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 capabilities allow.

For an approved list of ciphers, protocols, and signing criteria related to VPN configurations, refer to STD-SEC031A, Encryption Configurations and Product Standards for Commonwealth Data.

To ensure the protection of sensitive information, Agencies shall conform to the NIST Cryptographic Module Validation Program (CMVP) for encryption products and solutions.

As currently designed, neither Microsoft Team Foundation Server nor Azure DevOps satisfies the current CMVP Federal Information Processing Standards (FIPS) 140-2 implementation guidance. Agencies utilizing either Microsoft Team Foundation Server or Azure DevOps are not required to submit policy exceptions against this policy to utilize these solutions for testing environments so long as no Class "C" or Closed Records are maintained, stored, or transmitted within the solutions.

### 4.2 Data at Rest

Encryption shall be used to protect Class "C" or Closed Records at rest as defined by the *Data Classification Policy* and as outlined in *ITP-SEC019,* Policy and Procedures for Protection Commonwealth Electronic Data. 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, approved mobile and approved portable devices shall utilize encryption and shall not be placed in suspend mode when unattended. When not in use or unattended, such devices shall be shut down completely.

Agencies shall utilize the following types of encryptions for Data at Rest:

- Full Disk Encryption
- Volume Level Encryption
- File Encryption
- Data Element Encryption

#### 4.2.1 Full Disk Encryption

Full Disk Encryption shall be used on computers or computing devices storing Class "C" 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" 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" or Closed Records as defined in the *Data Classification Policy*.

#### 4.2.2 Volume Level Encryption

In cases where the volume contains Class "C" 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 devices shall use at least Volume Level Encryption.

#### 4.2.3 File Encryption

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

#### 4.2.4 Data Element Encryption

Data Element Encryption shall be used when Class "C" or Closed Records are stored in accordance with the *Data Classification Policy*. 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" or Closed Records.

### 4.3 Email Encryption

Authorized Users shall use the enterprise standard for secure email when sending outbound data transmissions via email that contain sensitive, protected, privileged or prerequisite-required information (also referred to as Class "C" records or Closed Records) as classified by the data owner that meets the criteria for encryption. Refer to the Data Classification Policy for policy guidelines on identifying, classifying, and encrypting Class "C" or Closed Records. Current enterprise email encryption product standards are outlined in the *Encryption Standard*.

An Email Encryption User Guide can be found on the IT Central Enterprise Messaging page under Email Encryption. The user guide explains how to send and read/view an encrypted email message.
Authorized users shall not send or forward encrypted work-related emails to their personal email account(s) per *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

Agencies shall refer to specific policies, statues, laws, or regulations including, but not limited to, Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act of 2002, the Gramm-Leach-Bliley Act of 1999 (GLBA), Internal Revenue Service (IRS), or Criminal Justice Information Services (CJIS) that involve data security where applicable to specific Agency business requirements to ensure the adequate protection of Commonwealth data.

#### 4.3.1 Monitoring

In accordance with *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*, encrypted email communications may be audited by the Enterprise Information Security Office (EISO) on a random basis to ensure compliance with appropriate policies, statues, laws, and regulations.

#### 4.3.2 Revisions/Updates

The Office of Administration, Office for Information Technology (OA/IT) reserves the right to update or revise the email encryption policy or implement additional policies in the future. Authorized Users are responsible for staying informed about Commonwealth policies regarding the use of IT resources and complying with all applicable policies.

#### 4.3.3 Examples of Sensitive Information Requiring Secure Email

##### 4.3.3.1 Protected Data

Includes, but is not limited to, protected health information, Social Security Administration numbers, credit card numbers, financial account numbers, and other information protected by HIPAA, GLBA, and other laws and regulations.

##### 4.3.3.2 Financial Information Data

Includes personally identifiable financial information, as defined in the GLBA, that is a combination of personally identifiable information (name, account number, etc.), with financial information relating to that individual (such as stock prices, investment options or borrowing arrangements), or credit card information. Financial information may include permissible, but prematurely released information, such as earnings statements, acquisition details, and quarterly statements.

##### 4.3.3.3 Intellectual Property Data

Information about Commonwealth intellectual property that may not be ready

for public release. E-mails that contain Intellectual Property Data may include terms and phrases such as design patent, trademark, or invention.

#### 4.3.3.4 Protected Health Information (PHI) Data

Electronic PHI data as defined in HIPAA includes individually identifiable information that relates to a person's health, mental or physical health treatment, or payment for healthcare services. Examples of PHI include any combination of personally identifiable information (such as patient name, account number or other identifying information) and healthcare treatment information (such as an ICD-9 diagnosis code, an American Medical Association treatment code, or the names of diseases or other health conditions).

#### 4.3.3.5 Criminal Justice Information (CJI)

CJI is the abstract term used to refer to all of the data necessary for criminal justice agencies to perform their mission and enforce the laws, including, but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to data necessary for any agency to perform their mission; including, but not limited to, data used to make hiring decisions.

#### 4.3.3.6 Personally Identifiable Information (PII)

PII is information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name or biometric records; and any other information that is linked or linkable to a specific individual, such medical, educational, financial, and employment information. In addition, driver's license number, state identification number, passport number and username or email, in combination with a password or security question and answer.

## 5. Contact

Questions or comments may be directed via email to OA, IT Policy.

## 6. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the enterprise IT policy exception process. Refer to the *IT Policy Governance Policy* for guidance.

## 7. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

| Version | Date | Purpose of Revision |
|---|---|---|
| Original | 01/06/2025 | Base Document |