Information Technology Policy
Enterprise Email Encryption

Number ITP-SEC008	**Effective Date** March 1, 2006
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** July 2024

1. Purpose

This Information Technology Policy (ITP) establishes the policy and enterprise-wide standards for secure email. Secure email shall be used by Authorized Users who have valid business requirements for sending emails containing sensitive information securely to third parties, business partners, and non-commonwealth entities. Secure email provides many key benefits to the Authorized User including, but not limited to:

- Protecting and encrypting all outbound emails where the email contents contain sensitive, protected, privileged or prerequisite-required information.
- Enabling agencies to comply with federal mandates requiring secure email transmissions.
- Ensuring that sensitive communications and exchange of information originating from the Commonwealth is not compromised.
- Decrypting secure messages received by external Commonwealth email recipients.

2. Scope

This ITP 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").

3. Objective

To establish policy and standards for enterprise-wide secure email encryption.

4. Policy

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 ITP-INF015 *Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data* and *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data* for policy guidelines on identifying, classifying, and encrypting Class "C" or Closed Records.

Current enterprise email encryption product standards are outlined in *STD-SEC008A, Enterprise Email Product Standards (Authorized CWOPA user access only)*.

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.

4.1 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.

4.2 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 Examples of Sensitive Information Requiring Secure Email

4.3.1 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.

4.3.2 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 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.

4.3.4 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).

4.3.5 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.

4.3.6 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. Responsibilities

5.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

5.2 Office of Administration, Office for Information Technology 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-ACC001 – Digital Accessibility Policy*
- *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data*
- *STD-SEC008A, Enterprise Email Encryption Product Standards (Authorized CWOPA user access only)*
- *ITP-SEC025, Proper Use and Disclosure of Personally Identifiable Information (PII)*
- *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*
- *ITP-SEC031, Encryption Standards*
- *Microsoft Purview Message Encryption User Guide*

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 shall 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 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	10/16/2009	Base Policy	N/A
Revision	12/10/2009	The references to automatic email encryption for outbound email have been removed and SEC008B has been rescinded.	N/A
Revision	9/17/2010	A reference added for non-commonwealth employees to receive secure emails from the commonwealth due to business requirements	N/A
Revision	4/2/2014	ITP Reformat	N/A
Revision	4/29/2015	Removed Microsoft Outlook XP and 2007 from Platforms in Current Standards table; replaced with "Current commonwealth-supported email solution"	N/A
Revision	4/07/2021	Updated Current Standards section Added Exemption Section added	N/A

Version	Date	Purpose of Revision	Redline Link
		Secure email definition added HIPAA and GLBA added to Policy Section CJI and PII added to Policy Section	
Revision	06/15/22	ITP refresh Moved standards to STD-SEC008A Replaced information regarding training with link to user guide Clarified language around forwarding encrypted email	N/A
Revision	07/26/2023	Scope updated based on connection to Commonwealth Network. Added references to Class "C" or closed records. Added references to ITP-INF015 and ITP-INF019 in policy language. Updated references to STD-SEC008A to include link to IT Central. Added references to IRS and CJIS as applicable regulations requiring encryption of email data. Expanded identifying information to include driver's license number, state ID number, passport number, username, or email, in combination with a password or security question/answer. Email Encryption User Guide was updated based upon the new name. New guide was published to IT Central and links in policy updated. Added ITP-SEC025 as reference document.	Revised IT Policy Redline <07/26/2023>