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** June 2023

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 employees. Secure email provides a number of 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 will not be 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 (hereinafter referred to as "agencies"). Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Definitions

3.1 Secure email: Involves encrypting, or disguising, the content of email messages to protect potentially sensitive information from being read by anyone other than the intended recipients.

4. Objective

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

5. Policy

Commonwealth Authorized Users are to use the enterprise standard for secure email when sending outbound data transmissions via email that contain sensitive, protected, privileged or prerequisite-required information classified by the data owner that meets the criteria for encryption. A listing of enterprise email encryption product standards can be found in STD-SEC008A *Enterprise Email Product Standards*.

- A user guide for email encryption can be found on IT Central at Encryption. The user guide explains how to send an encrypted email and how to read or view an encrypted message.

- Authorized users shall not send or forward encrypted emails to their personal email account(s) per Management Directive 205.34 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

- Refer to ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data* to determine the classification.

- Also, refer to specific laws 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), and any other law or regulation that involves data security.

5.1 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 set policies.

5.2 Revisions/Updates

Office of Administration, 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 computer and network resources and complying with all applicable policies.

5.3 Examples of Sensitive Information Requiring Secure Email

a. 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.

b. Financial Information Data: Includes personally identifiable financial information, as defined in the GLBA, that is a combination of a 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.

c. **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.

d. **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).

e. **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.

f. **Personnel Identifiable Information (PII):** PII is information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

6. Responsibilities

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

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

7. 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-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data*
- ITP-SEC031 *Encryption Standards*

- STD-SEC008A Enterprise Email Encryption Product Standards

8. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

9. 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.

10. 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 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 Secure email definition added HIPAA and GLBA added to Policy Section CJI and PII added to Policy Section	N/A
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	Revised IT Policy Redline <06/15/2021>