pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Enterprise E-mail Encryption

ITP Number	***Effective Date***
ITP-SEC008	March 1, 2006
Category	***Supersedes***
Security	
Contact	***Scheduled Review***
ra-oaitb@pa.gov	April 2022

1. Purpose

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

- Protecting and encrypting all outbound e-mails where the e-mail contents contain sensitive, protected, privileged or prerequisite-required information.

- Enabling agencies to comply with federal mandates requiring secure e-mail transmissions.

- Ensuring that sensitive communications and exchange of information originating from the Commonwealth will not be compromised.

- Decrypting secure messages received by external Commonwealth e-mail 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. Objective

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

4. Definitions

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

5. Policy

Commonwealth Authorized Users are to use the enterprise standard for secure e-mail when sending outbound data transmissions via e-mail that contain sensitive, protected, privileged or prerequisite-required information classified by the data owner that meets the criteria for encryption.

- E-mail encryption training will be provided by the e-LMS Web-based training program. The training involves the use of the send secure button, how to use a subject line to secure an e-mail, and how to create a user account in the e-mail encryption portal.
- Outbound encrypted e-mails will not be permitted to be forwarded to personal e-mail accounts.

- 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.

Monitoring

In accordance with Management Directive 205.34 Amended, *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*, encrypted e-mail communications may be audited by the Enterprise Information Security Office on a random basis to ensure compliance with set policies.

Revisions / Updates

Office of Administration, Office for Information Technology (OA/OIT) reserves the right to update or revise the e-mail 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.

Examples of Sensitive Information Requiring Secure E-Mail

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.

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.

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.

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).

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.

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. Standards

CURRENT STANDARDS

(These technologies meet the requirements of the current architecture and are recommended for use.)

Technology	Platforms	Technology Classification
Microsoft O365 Message Encryption	Microsoft Azure Rights Management (Azure RMS) which is part of Azure Information Protection	Current

CONTAIN

(These technologies no longer meet the requirements of the current architecture and are not recommended for use. These technologies are to be phased out over time. No date has been set for their discontinuance.)

Technology	Platforms	Technology Classification
--	--	Contain

RETIRE

(These technologies are being phased out. Plans are to be developed for their replacement, especially if there is risk involved, such as lack of vendor support. A date for retirement has been set.)

Technology	Platforms	Technology Classification
--	--	Retire

EMERGING / RESEARCH

(Emerging technologies have the potential to become current standards. At the present time, they are to be used only in pilot or test environments where they can be evaluated. Use of these technologies is restricted to a limited production mode and requires approval of a waiver request. Research technologies are less widely accepted, and time will determine if they become a standard.)

Technology	Platforms	Technology Classification
--	--	Emerging / Research

7. Related ITPs/Other References

- MD 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*

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 Waiver Review Process* for guidance.

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

Version	Date	Purpose of Revision	Redline Link
Original	10/16/2009	Base Policy	
Revision	12/10/2009	The references to automatic email encryption for outbound email have been removed and SEC008B has been rescinded.	
Revision	9/17/2010	A reference added for non-commonwealth employees to receive secure emails from the commonwealth due to business requirements	
Revision	4/2/2014	ITP Reformat	
Revision	4/29/2015	Removed Microsoft Outlook XP and 2007 from Platforms in Current Standards table; replaced with "Current commonwealth-supported email solution"	
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	Revised IT Policy Redline <4/07/2021>