pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Enterprise E-mail Encryption

ITP Number	***Effective Date***
ITP-SEC008	March 1, 2006
Category	***Supersedes***
Recommended Policy	
Contact	***Scheduled Review***
ra-oaitb@pa.gov	Annual

This Information Technology Policy (ITP) establishes policy and enterprise-wide standards for secure e-mail.

1. Purpose

Secure e-mail addresses the needs of commonwealth e-mail authorized users who have valid business requirements for sending e-mails containing sensitive information securely to third parties, business partners, and non-commonwealth employees. This Information Technology Policy (ITP) establishes the policy and enterprise-wide standards for secure e-mail. Secure e-mail provides a number of key benefits to the commonwealth e-mail authorized user community including:

- Protecting and encrypting all outbound e-mails where the e-mail contents contain sensitive 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 Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. 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. 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 information or 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 or 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.

Monitoring

In accordance with the Commonwealth of Pennsylvania Information Technology Acceptable Use Policy, Management Directive 205.34, CoPA Information Technology Acceptable Use Policy, encrypted e-mail communications may be audited by the Office for Information Security 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

Sensitive Data: Protected health information, Social Security Administration numbers, credit card numbers, financial account numbers, and other information protected by the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and other laws and regulations.

- Refer to ITP-SEC019 Policy and Procedures for Protecting Commonwealth Electronic Data, to determine the classification.
- Mandates of law including, but not limited to HIPAA, Sarbanes-Oxley Act of 2002, the GLBA, and any other law or regulation that involves data security.

Financial Information Data: Personally identifiable financial information, as defined in the GLBA that is either a combination of a personal identifier (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 data may include permissible, but prematurely released information, such as earnings statements, acquisition details, and quarterly statements.

Intellectual Property Data: E-mail that contains information about commonwealth intellectual property that may not be ready for public release might 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 personal identifiers (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.

5. Standards

CURRENT STANDARDS

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

Technology	Platforms	Technology Classification
IronPort (Cisco) - Outbound e-mail encryption	Current commonwealth-supported email solution	Current
Microsoft Exchange 2007 – Internal e-mail encryption using TLS	Microsoft Outlook 2007	Current

CONTAIN

(These technologies no longer meet the requirements of the current architecture and are not recommended for use. They 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 mm/dd/yy

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 will become a standard.)

Technology	Platforms	Technology Classification
--	--	Emerging / Research

6. Related ITPs/Other References

- MD 205.34 - *CoPA Information Technology Acceptable Use Policy*
- ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*

7. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

8. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

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

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