pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Encryption Standards for Data in Transit

ITP Number	***Effective Date***
ITP-SEC031	August 17, 2007
Category	***Supersedes***
Recommended Policy	
Contact	***Scheduled Review***
RA-ITCentral@pa.gov	Annual

This Information Technology Policy (ITP) establishes policy and standards for encryption of data in transit.

1. Purpose

The purpose of this Information Technology Policy (ITP) is to improve the confidentiality and integrity of data in transit by prescribing the use of encryption.

The Commonwealth of Pennsylvania is a trusted steward of information. Many solutions and technologies have been put in place to improve connectivity and sharing between commonwealth entities with external business partners and citizens.

Data in transit is any type of information that is transmitted between systems, applications, or locations. Encryption of data in transit is a critical mechanism to protect that data. Unauthorized disclosure or alteration of data in transit could cause perceivable damage. Criteria to be taken into account when encrypting data in transit include:

- Data sensitivity - Refer to ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data,* to determine the classification of sensitive, protected or exempt data.

- Mandates of law including, but not limited to, 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 security in transit.

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. Policy

Agencies are to protect the transmission of sensitive, protected, or exempt data as determined by SEC019. Agencies are to adhere to the Advanced Encryption Standard (AES) for symmetric encryption. For asymmetric encryption, agencies are to follow ITP-SEC013 - *Identity Protection and Access Management (IPAM) Architectural Standard - Identity Management Services,* and ITP-SEC014 - *IPAM Architectural Standard – Identity Management Technology Standards.*

Internet Protocol Security (IPSec) gateway to gateway implementations utilizing triple data encryption standard (3DES) is to be migrated to IPSec/AES to take advantage of increased security; new IPSec implementations are not to use 3DES.

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 are considered to be secure.

Agencies are strongly recommended to utilize 256-bit key sizes, and hashing algorithms that utilize 160-bit (or greater) digest lengths. Agencies are encouraged to use larger key/digest sizes where performance and client constraints allow.

Encryption products used to protect sensitive information are to conform to the NIST Cryptographic Module Validation Program listing http:/csrc.nist.gov/cryptval/.

Transmission Mechanism Examples	Meets ITP-SEC031
HTTPS in export mode (40-bit keys)	No, does not meet key size requirements, and does not utilize AES.
HTTPS (TLS 1.0, AES 128, 192, or 256)	Yes
Secure Shell (SSH)-1	No, SSH-1 does not utilize AES encryption.
SSH-2 (DES, 3DES, or Blowfish)	No, these algorithms are not AES.
SSH-2 (AES)	Yes
SCP/SFTP over SSH-2	Yes
HTTP over SSH-2	Yes
VPN Clients (TLS 1.0, passwords or PKI certificates)	Yes
IPSec (3DES for encryption)	No, IPSec/3DES setups are to be migrated to IPSec/AES.
IPSec (AES-CBC for encryption)	Yes
Layer 2 Forwarding (L2F) or Point-to-Point Tunneling Protocol (PPTP)	No, L2F and PPTP do not offer encryption.
HTTPS (TLS 1.0, AES 128, 192, or 256) over L2F or PPTP	Yes, L2F/PPTP is transporting encrypted traffic.

4. References

- ITP-SEC013 - *Identity Protection and Access Management (IPAM) Architectural Standard - Identity Management Services*
- ITP-SEC014 - *IPAM Architectural Standard – Identity Management Technology Standards*
- ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*

5. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

6. 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	8/17/2009	Base Policy
	9/17/2009	Rewrote policy section and added transmission mechanism table
	4/2/2014	ITP Reformat