pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Encryption Standards for Data in Transit

ITP Number ITP-SEC031	**Effective Date** August 17, 2007
Category Security	**Supersedes** --
Contact RA-ITCentral@pa.gov	**Scheduled Review** October 2018

1. Purpose

Improve the confidentiality and integrity of data in transit by prescribing the use of encryption.

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 ITP-SEC019. 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.

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 security, protected, privileged or prerequisite-required information.

- 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.

The Commonwealth Metropolitan Area Network (MAN) should not be considered a trusted mode of transit (i.e. zero trust network) and all data traffic through the MAN and commonwealth agency networks should be considered untrusted unless additional interagency traffic encrypted trusts are established and maintained. Agencies must comply with all Security IT policy guidance to properly secure all commonwealth data in transit.

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 as detailed in this policy 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/groups/STM/cmvp/.

Transmission Mechanism Examples	**Meets ITP-SEC031**
HTTPS in export grade ciphers (40-bit and 56-bit keys)	No, does not meet key size requirements, and does not utilize AES.
Rivest Cipher 4 (RC4)	No
HTTPS (any SSL version, TLS 1.0, 1.1, 3DES)	Contain only. New deployments require a COPPAR waiver approval.
HTTPS (TLS 1.2, 1.3, AES 128 bit or higher) HTTPS (TLS 1.2, 1.3, AES 128 bit or higher) over L2F or PPTP	Yes
Secure Shell (SSH)-1	No, SSH-1 does not utilize AES encryption.
SSH-2 (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 1.1, 1.2 (preferred), passwords or PKI	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.
SHA-1 cipher for certificate signing	Contain. Existing SHA-1 ciphers will cease to function past February 2017 in current web browsers (Microsoft Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox)
SHA-2 family of ciphers for certificate signing (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256)	Yes
SHA-3 family of ciphers for certificate signing (SHA3-224, SHA3-256, SHA3-384, SHA3-512; XOFs: SHAKE128, SHAKE256)	Yes

4. References

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 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- ITP-SEC000 – *Information Security Policy*
- 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*
- ITP-SEC020 - *Encryption Standards for Data at Rest*
- ITP-SFT005 - *Managed File Transfer (MFT)*

5. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

6. Publication Version Control

It is the 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.

7. Exemption from this Policy

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required.

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

Version	Date	Purpose of Revision
Original	08/17/2009	Base Policy
Revision	09/17/2009	Rewrote policy section and added transmission mechanism table
Revision	04/02/2014	ITP Reformat
Revision	08/17/2015	Revised Data sensitivity classification categories language regarding SEC019
Revision	12/09/2016	• Revised Transmission Mechanism Examples table with updated encryption protocol requirements • Added Exemption section • Added ITP-SEC000 reference • Revised NIST Cryptographic Module Validation Program URL • Added Secure Hash Algorithm (SHA) language
Revision	10/24/2017	• Added statement on "untrusted network" of Commonwealth MAN and agency networks in Policy section • Added additional References • Moved language from Purpose to Policy section for clarity