pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Managed File Transfer (MFT)

ITP Number	**Effective Date**
ITP-SFT005	February 22, 2017
Category	**Supersedes**
Software	None
Contact	**Scheduled Review**
RA-ITCentral@pa.gov	February 2018

1. Purpose

The purpose of this Information Technology policy (ITP) is to establish an enterprise-wide policy for the use of Managed File Transfer by the Commonwealth, its business partners, and the public to exchange files and data securely in various formats that are too large to be transferred via e-mail.

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. Background

There is a need across the commonwealth to securely transfer large volumes of data across agencies, business partners, and customers. While FTP was used in the past, the technology was not designed to be a secure protocol, nor on its own, provide a way to secure or manage the payload or the transmission. With security and compliance in mind, MFT does more than simply secure files while being transferred. MFT manages the secure transfer of data from one computer to another through a network and offers a higher level of security and control than FTP, along with an increased focus on auditing, records management, and security.

4. Definitions

4.1 Managed File Transfer (MFT): manages the secure transfer of data from one computer to another through a network and offers a higher level security and control than FTP. MFT is characterized by having all or most of the following features:

- Support multiple file transfer protocols including FTP/S, OFTP, SFTP, SCP, AS2, and HTTP/S.
- Securely transfer files over public and private networks using encrypted file transfer protocols.
- Securely store files using multiple data encryption methods
- Automate file transfer processes between trading partners and exchanges including detection and handling of failed file transfers.
- Authenticate users against existing user repositories such as LDAP and Active Directory
- Integrate to existing applications using documented APIs (application programming interfaces)
- Generate detailed reports on user and file transfer activity.

5. Objective

The objective of this policy is the protection of critical and sensitive electronic data whether at rest or in transit. The commonwealth is equally committed to protecting electronic data from accidental or intentional intrusion while preserving the information sharing requirements and business needs across the commonwealth.

6. Policy

Agencies are to review the enterprise MFT service offering located at IT Central and contact the Office of Administration/Office for Information Technology at ra-enterprisemftserv@pa.gov to discuss options for the use of the service.

Any agency that has its own FTP service shall develop a transition plan to migrate FTP to MFT capabilities, and submit an exemption as set forth in this ITP.

Additionally, anonymous FTP allows anyone with an Internet connection to access FTP connections to the site, including uploading or downloading files, without having to log in with a username and password. Anonymous FTP on the Internet has been identified as a security risk to the commonwealth, and as such shall not be made available without seeking an exemption as set forth in this ITP. Any agency that has its own Internet-accessible FTP server shall remove anonymous FTP capability immediately or submit an exemption request for continued use.

An agency providing files that are public facing must understand the sensitivity requirements and protections that the data requires. If the data contains any sensitive data or data covered under the Pennsylvania Data Breach Notification Act, the data must be encrypted and hosted on a MFT capable server.

All public facing sites must contain a banner indicating a warning to all end users indicating the acceptable use of the site relating to the posting of sensitive information.

Public facing MFT or FTP sites are not to be used for the distribution of commercial software that requires a valid license for use.

FTP servers containing exemptions from this policy are subject to random assessments by the Office of Administration/Office for Information Technology in order to mitigate risks to the commonwealth's security posture.

7. Responsibilities

- Data Owner - It is essential to identify sensitive, protected, and exempt data.
- Data Owner – All files residing on MFT and/or FTP servers are managed, retained, and disposed of in conformance with approved records retention and disposition schedules.
- Service Provider - Protection of critical and sensitive electronic data at rest or in transit.

8. Related ITPs/Other 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*
- MD 210.5 *State Records Management Program*
- ITP-BUS004 *IT Waiver Review Process*
- ITP-PLT005 *Intel Based Server Operating System*
- ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data*
- ITP-SEC020 *Encryption Standards for Data at Rest*
- ITP-SEC031 *Encryption Standards for Data in Transit*
- ITP-SFT000 *Software Development Life Cycle (SDLC) Policy*
- ITP-SYM006 *Desktop and Server Software Patching*
- Enterprise Service Catalog: https://itcentral.pa.gov/Pages/Enterprise-Services.aspx (Limited Access)

9. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

10. 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.

11. 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	02/22/2017	Base document Moved to Software domain from Application, including ITP number change Replaces ITP-APP031 *File Transfer Protocol* ITP