Information Technology Policy
Managed File Transfer (MFT)

Number
ITP-SFT005

Effective Date
February 22, 2017

Category
Software

Supersedes
None

Contact
RA-ITCentral@pa.gov

Scheduled Review
January 2023

1. Purpose

This Information Technology policy (ITP) establishes an enterprise-wide policy for the use of the Global Managed File Transfer (MFT) 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 ITP applies to all departments, offices, 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.

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP that are applicable to the products and services provided to the Commonwealth.

3. Background

There is a need across the Commonwealth to securely transfer large volumes of data across agencies, business partners, and customers. While File Transfer Protocol (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 (*to be published to online Policy Glossary*)

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 of 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, SFTP, 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 third-party vendors, licensors, contractors, or suppliers and exchanges including detection and handling of failed file transfers.
- Authenticate users against existing user repositories internal and external (Lightweight Directory Access Protocol (LDAP) and Active Directory (AD)).
- Integrate to existing applications using documented Application Programming Interfaces (APIs).
- Generate detailed reports on user and file transfer activity.

4.2 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.

5. Objective

The objective of this policy is to protect electronic data from accidental or intentional breach while preserving the information sharing requirements and business needs across the Commonwealth by driving the adoption of MFT, which offers a higher level of security and control than FTP.

6. Policy

Agencies shall review the enterprise MFT service offering located at IT Central and contact the Office of Administration/Office for Information Technology (OA/OIT) at ra-enterpriseftpserv@pa.gov to discuss options for the use of the service.

Any agency that chooses to use its own FTP service rather than the enterprise MFT service, must obtain an approved IT Policy waiver against this policy.

Anonymous FTP on the Internet has been identified as a security risk to the Commonwealth, and as such, shall not be made available without an approved IT Policy waiver against this policy. Any agency that has its own Internet-accessible FTP server shall remove anonymous FTP capability immediately or submit an IT Policy waiver request for continued use.

Agencies shall ensure that if they are providing any sensitive data or data covered under the Pennsylvania Data Breach Notification Act, the data shall be encrypted and hosted on a MFT capable server.

All public facing sites shall contain a banner warning all end users regarding the acceptable use of the site and 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 OA/OIT in order to mitigate risks to the Commonwealth's security posture.

EDC performs random scans on internet facing MFT and FTP sites.

7. Responsibilities

7.1 Agencies shall

- Identify sensitive, protected, and exempt data.
- Manage, retain, and dispose of all files residing on MFT and/or FTP servers in conformance with approved records retention and disposition schedules.
- Collaborate with Third-party vendors to gather requirements prior to submitting a request to transfer or receive electronic data via FTP or MFT servers.

7.2 OA/OIT shall

- Protect critical and sensitive electronic data at rest or in transit as identified by the Agency.
- Discuss enterprise MFT service offering options, review requirements and provide guidance to the Agencies.
- Configure services only to accept a certain level of encryption from the third-party vendor.

7.2.1 EISO Shall

Perform random security assessments.

7.3 Third-party vendors, licensors, contractors, or suppliers shall

Collaborate with the Agency to gather requirements prior to being able to transfer or receive electronic data via FTP or MFT servers.

8. Related ITPs/Other References

Definitions of associated terms of this policy are published on the Office of Administration's public portal:
http://www.oa.pa.gov/Policies/Pages/Glossary.aspx

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 Amended *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- Management Directive 210.5 Amended *the Commonwealth of Pennsylvania State Records Management Program*
- ITP-BUS004 *IT Policy Waiver Review Process*
- ITP-PLT005 *Server Operating System Policy*
- ITP-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data*
- ITP-SEC031 *Encryption Standards*

- ITP-SFT000 *Software Development Life Cycle (SDLC) Policy*
- ITP-SYM006 *Commonwealth IT Resources Patching Policy*
- Pennsylvania Breach of Personal Information Notification Act, Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301—2329 (P.L. 474, No. 94, 2005),
- 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 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.

11. 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 Policy Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original		• Base document • Moved to Software domain from Application, including ITP number change • Replaces ITP-APP031 File Transfer Protocol ITP	
Revision	01/19/2022	• ITP Refresh • Updated to accessible ITP template • Added Third-party vendors to Scope and Responsibilities • Updated resource account for the Enterprise MFT group • Updated policy to further describe when an Agency needs to submit an IT Policy Waiver • Updated Responsibilities, Related ITPs/Other References, and Exemption Sections • Added links	Revised IT Policy Redline <01/19/2022>