

---

# Information Technology Policy

---

## *File Transfer Protocol (FTP) Policy*

<b><i>ITP Number</i></b> ITP-APP031	<b><i>Effective Date</i></b> November 20, 2009
<b><i>Category</i></b> Recommended Policy	<b><i>Supersedes</i></b>
<b><i>Contact</i></b> <a href="mailto:RA-itcentral@pa.gov">RA-itcentral@pa.gov</a>	<b><i>Scheduled Review</i></b> April 2015

**This Information Technology Policy (ITP) establishes enterprise-wide policy for the use of a File Transfer Protocol (FTP) server.**

### 1. Purpose

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

### 2. Background

Use of the enterprise FTP file servers are available to all agencies that are attached to the Metropolitan Area Network (MAN). The Internet FTP file server is accessible to the commonwealth business partners. Agencies may also set up and use their own FTP servers following the established policies noted in this ITP.

### 3. 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.

### 4. Policy

The Commonwealth is committed to the protection of critical and sensitive electronic data whether at rest or in transit. Refer to ITP-SEC020 - *Encryption Standards for Data at Rest*, and ITP-SEC031 - *Encryption Standards for Data in Transit*. It is essential to identify sensitive, protected, and exempt data

according to the procedures set forth in ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*.

The commonwealth is equally committed to protecting electronic data from accidental or intentional intrusion while preserving the information-sharing requirements and needs of the agencies.

Agencies are to contact the Office of Administration/Office for Information Technology/Bureau of Infrastructure and Operations (OA/OIT/BIO) [ra-enterpriseftpserv@pa.gov](mailto:ra-enterpriseftpserv@pa.gov) to discuss options for the use of enterprise and/or agency-hosted FTP servers. If the agency has a business need to provide public (Internet) FTP access, a waiver is to be completed and submitted the ITP-PRO001 - Procurement Review Process. Requests are to be entered into the COPPAR Tool located at [coppa.oa.pa.gov/](http://coppa.oa.pa.gov/). Agency CIO approval is required. Agencies that have existing Internet servers are to ensure that all security policies identified in this ITP are followed.

### **Anonymous FTP**

Anonymous FTP allows anyone with an Internet connection to access FTP connections to your 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. The commonwealth will not make anonymous FTP available via the enterprise FTP server. However, if an agency requires anonymous FTP access to meet a specific business need, the agency may seek an exemption as set forth in this ITP.

Any agency that has its own Internet-accessible FTP server should remove anonymous FTP capability immediately or submit a waiver request for continued use.

### **Acceptable Use:**

An agency hosting files on a commonwealth public facing FTP server or having files posted on any public facing FTP server on its behalf must understand the sensitivity requirements and protections that the data requires (as set forth in ITP-SEC019, ITP-SEC020, and ITP-SEC031). If the data contains any sensitive data or data covered under the Pennsylvania Data Breach Notification Act, the data must be encrypted before it will be hosted on the FTP site.

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

Section 5 of this ITP provides a description of enterprise FTP services and the procedure to obtain enterprise FTP services available from OA/OIT/BIO to agencies.

Section 6 of this ITP details the requirements and procedures for agencies desiring to host and configure an Intranet FTP server.

**5. Enterprise File Transfer Protocol (FTP) Guidelines**

Enterprise File Transfer Protocol (FTP) servers are maintained by the Office of Administration/Office for Information Technology/Bureau of Infrastructure and Operations (OA/OIT/BIO).

OA/OIT/BIO offers the following enterprise FTP services:

Services	File Encryption	Data Retention	Data Backup
Internet FTP	Yes	Thirty (30) days on FTP Server	--
Intranet FTP	Yes	Thirty (30) days on FTP Server	One (1) year

Agencies requesting OA/OIT/BIO-hosted enterprise Internet FTP services are to complete and e-mail the attached *Enterprise Internet FTP Access with File Encryption Form* to OA/OIT/BIO at [ra-enterpriseftpserv@pa.gov](mailto:ra-enterpriseftpserv@pa.gov).

Agencies requesting OA/OIT/BIO-hosted enterprise Intranet FTP services are to complete and e-mail the attached *Enterprise Intranet FTP Access Form* to OA/OIT/BIO at [ra-enterpriseftpserv@pa.gov](mailto:ra-enterpriseftpserv@pa.gov).

**6. Agency Intranet File Transfer Protocol (FTP) Guidelines**

Agencies are to request approval to host an FTP server by completing and e-mailing the attached Agency Intranet FTP Access Form to Office of Administration/Office for Information Technology/Bureau of Infrastructure and Operations (OA/OIT/BIO) [ra-enterpriseftpserv@pa.gov](mailto:ra-enterpriseftpserv@pa.gov).

In addition to the above requirement, agencies are to follow the following policies to establish an Intranet FTP server.

- Follow ITP-APP002 - *Web Server/Application Server Standards*.
- The FTP server is to have current patches and security fixes installed as per the ITP-SYM006 - *Desktop and Server Software Patching Policy*.
- The FTP server is to have a supported operating system (OS) as provided per ITP-PLT005 – *Intel Based Server Operating System Policy*.
- 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*

A complete list of CERT recommendations for anonymous FTP servers is provided in the Anonymous FTP Configuration Guidelines. Contact [ra-enterpriseftpserv@pa.gov](mailto:ra-enterpriseftpserv@pa.gov) to obtain a copy.

Approved FTP servers are to be configured using industry best practice hardening guidelines and are subject to assessment by the Chief Information Security office.

## 7. Related ITPs/Other References

- ITP-PRO001 – *IT Procurement Review Process*
- ITP-APP002 - *Web Server/Application Server Standards*
- ITP-SYM006 - *Desktop and Server Software Patching Policy*
- ITP-PLT005 – *Intel Based Server Operating System Policy*
- 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*

## 8. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

## 9. 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](mailto:RA-itcentral@pa.gov).

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

Version	Date	Purpose of Revision
Original	11/20/2009	Base Document
	10/25/2010	ITB Refresh
	03/28/2012	ITB additions
	4/2/2014	ITP Reformat; Merged OPD-APP031A, OPD-APP031B into ITP