Office of the Chief Information Officer Directive: IT 10.06

Chapter: Network Security

Subject: File Transfer Protocol (FTP)

Issued: 04/2019 Last

Review: 01/2024

1 DIRECTIVE

1.01 An FTP server that allows user access from an unsecure network such as the Internet must be restricted to public, non-private data content only, and be configured as follows:

- (a) The server must allow anonymous login only.
- (b) The server must be restricted to read-only access. Connected users may not upload files to the FTP server.
- 1.02 An FTP server with user access restricted to a company's internal network may allow either anonymous login or user login. Anonymous login may be used only for company-wide shared libraries. User login must be used for controlling unrestricted access to workgroup libraries.
- 1.03 An FTP server that allows users to upload files to shared libraries must also caution the users that uploaded files are not protected and that the server cannot guarantee file backup.
- 1.04 All business requirements for secure file transfer functionality must use an FTP replacement application suite whenever the risk outweighs the benefits of FTP technology (i.e., free, easy-to-use, widely available).

2 PURPOSE

2.01 The purpose of this Directive is to ensure that implementation of an FTP server does not create a security risk for the data made available on the FTP site, and that the FTP site is not at risk from denial-of-service attacks.

3 SCOPE

This directive applies to all company servers and personal computers set up to provide an FTP service.

Office of the Chief Information Officer Directive: IT 10.06 | Issued: 04/2019

Chapter: Network Security

Subject: File Transfer Protocol (FTP)

Last Review: 01/2024

4 RESPONSIBILITY

4.01 **IT Planning** and IT Technical Support are responsible to establish an appropriate file transfer methodology suited to the overall security requirements of the enterprise.

- 4.02 IT Technical Support and IT Operations are responsible to configure all company file transfer servers to conform with this directive.
- 4.03 All employees who have authority to establish a file transfer server for workgroup use are responsible to configure the server to conform with this directive.

5 DEFINITIONS

None

6 RELATED DIRECTIVES

OCIO IT 1.01 - Strategic Planning

OCIO IT 1.02 - Tactical Planning

OCIO IT 1.05 – Risk Assessment

OCIO IT 8.03 - User Identification and Passwords

OCIO IT 8.04 - Confidentiality and Privacy

OCIO IT 9.03 - Data Access Controls

OCIO IT 9.06 – Data Encryption