UNIVERSITY OF CENTRAL FLORIDA

University Standards

Subject:	File Transfer and Processing Standards
Standards Number:	108
Effective Date:	November 8, 2019
Revised Date:	[First version]
Responsible Authority:	Information Security Office
Pages:	4

ACCOUNTABILITY/APPLICABILITY:

These standards apply to any UCF personnel that build, administer, or maintain any of the following systems:

- A UCF system that transfers data to another UCF System using a File Transfer protocol.
- A UCF system that "stages" or processes data prior to transferring it to its' ultimate destination.

STANDARDS STATEMENT:

Data transfers between UCF systems are common, both between systems within the UCF network(s) as well as between UCF systems and third-party systems on the internet. The security of these data transfers, both in terms of the data transfer as well as where the data is held at each stage of the transfer, is critical. This standard outlines technical requirements for UCF data transfers when using common protocols such as SFTP. It also addresses common areas of risk that can arise related to the overall data transfer process, such as retention standards and the approach to "intermediate" servers for processing or retrieval.

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476

STANDARDS:

1. Data Transfer Method

a. Data transfer methods that do not create intermediate "flat files" between the data source and destination server are always preferred. From a security perspective, the creation of intermediate flat files creates data hygiene overhead that invites security and compliance concerns if not closely managed. Instead of placing a file on an intermediate server for processing or retrieval, consider these first:
   - Transactional API's, such as REST HTTPS APIs
   - Direct SFTP to the destination server (no intermediate destination for retrieval)

2. SFTP Standards

a. **Encryption in Transit** SFTP is required for all data transfers involving Restricted or Highly Restricted Data, either internal to UCF network(s) or external. Unsecured FTP is not acceptable for Restricted or Highly Restricted Data.

b. Encryption at Rest Highly Restricted data must be encrypted at rest before sending, such as using PGP with a 4096-bit key.

c. **Authentication** SFTP connections should be authenticated using Public Key Authentication, or a strong username and password in accordance with the "Privileged Account" section of UCF Standard 501: Passwords Standards

3. Intermediate Transfer Servers and File Processing

The following standards apply to any data on an intermediate server between the source and destination, such as for processing or retrieval.

a. Retention

i. For Restricted and Highly Restricted Data, it is recommended that files on a processing server should be deleted as soon as they have been consumed by the destination.
   1. If there is a documented business reason for retention, such as for troubleshooting purposes, the standard retention period is **7 days**.
   2. Provided there is a documented business reason, exceptions to the 7 day period of up to **30 days** are acceptable.

ii. If there is a business need for longer retention, the files should be moved to a secured archive server elsewhere, such as a backup server or secured fileshare, that is separate from the data transfer pipeline and that has strict access controls and encryption at rest, where they can be retained for up to 90 days.

b. Encryption at Rest

i. Highly Restricted Data must remain encrypted at rest on the processing servers and archive server.

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

DEFINITIONS:

API: An Application Programming Interface is a protocol in place on a given system that provides a framework for clients to request data, and the server to return the requested data in a defined format. Modern APIs typically run over the web via HTTPS.

PGP: Pretty Good Privacy is a program that provides a means to encrypt data and send it confidentially.

Public Key Authentication: A means of authentication supported by SFTP and other protocols that uses a public and private key pair instead of a password. Users share their public keys with others that need access, while the private key is stored securely and kept secret. It is generally more robust and more secure than traditional passwords.

HTTPS: The secure version of the HyperText Transfer Protocol that encrypts traffic in transit.

SFTP: The SSH File Transfer Protocol provides a means to transfer files over the File Transfer Protocol in an encrypted manner.

RELATED DOCUMENTS: [Examples below:]

1. 4-008.1 *Data Classification and Protection* policy
2. UCF Information Security Policies: https://infosec.ucf.edu/policies-and-standards/
    a. 103 Server Security Standards
    b. 501: Passwords Standards
    c. 702 TLS/SSL Standards

CONTACTS:

Information Security Office https://infosec.ucf.edu infosec@ucf.edu	Security Incident Response Team (SIRT) https://infosec.ucf.edu/incident-response/ sirt@ucf.edu
Identity Access Management (IAM) https://infosec.ucf.edu/iam iam@ucf.edu	UCF IT Support Center (407) 823-5117 https://ucf.service-now.com/ucfit itsupport@ucf.edu

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution

HISTORY:

Revision Date	Summary of Change
November 8, 2019	First Version

INITIATING OFFICE: Information Security Office

STANDARDS APPROVAL
(For use by the Information Security Office)

Standards Number: *108*

Initiating Office: [Information Security Office]

Chief Information Security Officer: *Chris Vakhordjian*

Signature: chrisv Digitally signed by chrisv Date: 2019.11.12 10:21:03 -05'00' Date: _____

Division of Information Technologies & Resources
P.O. Box 162500 • Orlando, FL 32816-2500 • (407) 823-2711 • FAX (407) 823-5476
An Equal Opportunity and Affirmative Action Institution