Family Partnerships of Central Florida
BREVARD | ORANGE | OSCEOLA | SEMINOLE

PROCEDURE

Series:	**Information Technology**	**COA: RPM 5 CFOP: 50.2** **DCF Contract: GJ401**

Procedure Name:	Information Systems Data Back-Up, Restoration and Disposal
Procedure Number:	IT-801
Reviewed Date:	10/02/2025
Revision #/Date:	10/02/2025
Effective Date:	Replaces Existing IT801 & IT805 7/1/2008
Applicable to:	Family Partnerships of Central Florida (FPOCF)

Purpose: It is the procedure of Family Partnerships of Central Florida to routinely copy electronic data to alternate locations and devices to enable quick restoration in the event of a natural disaster, intentional destruction, systems malfunction, or operator error. FPOCF ensures that data integrity is maintained in the event that data has to be restored. Additionally, the MIS Director will implement the necessary disposal methods to guarantee that data is disposed of in a manner that ensures compliance with Health Insurance Portability and Accountability Act (HIPAA), Protected Health Information (PHI), and Confidentiality compliance.

Definitions:

Backup - A ***backup***, or ***data backup*** is a copy of computer ***data*** taken and stored elsewhere so that it may be used to restore the original after a ***data*** loss event.

Restore - A **restore** is performed to return **data** that has been lost, stolen or damaged to its original condition or to move **data** to a new location.

Full Backup - is a total copy of your organization's entire data assets, which backs up all your files into a single version.

Incremental Backup - An incremental **backup** covers all files that have been changed since the last **backup** was made, regardless of **the backup** type.

Differential Backup - a type of data **backup** that preserves data, saving only the difference in the data since the last full **backup**.

Procedure:

A. Workstations and End Users

1. All data used in conjunction with performing the duties of a position is the property of FPOCF and will be treated as a company owned resource.

2. All data will be stored in a location approved by FPOCF. MIS Director
3. Permanent storage of data in any other location or on removable media including but not restricted to Floppy disks, Compact Disks (CDs), Jump Drives (also known as Thumb Drives) is strictly prohibited.

4. Removable storage devices may be used for temporary storage. Confidential/HIPAA/PHI data may not be stored on any unencrypted mobile devices (laptops, thumb drives, CDs, disk, etc.).

5. End user data will be stored on one or more network servers. Workstations will not be backed up since no user-created data will be stored locally.

B. Servers

1. All user data on each FPOCF server is backed up on a ***4-hour*** basis to a separate physical disk or other media. Application servers are backed up every ***1-hour***.

2. In addition to localized backups, data is then replicated to a geographically diverse data center on a ***24-hour*** basis for additional Business Continuity protection.

C. Restoration

1. To request a restoration of backed-up data, the end user will send an email request through the FPOCF Helpdesk describing the extent of the loss and providing any details necessary for a successful restoration (i.e., shared drive where file resides, the folder name, the full file name and type, the last date and time file was known to exist, and the date and time the file was lost or destroyed).

D. Disposal

To appropriately and reasonably destroy and/or dispose of agency and client information, all FPOCF staff ensures equipment ensures compliance with HIPAA/PHI/Confidential disposal methods.

1. Computers:
   a. FPOCF shall use at minimum the standardized DoD-7 data destruction method executed from a CD to completely overwrite all data contained on the hard drive. FPOCF may remove the hard drive for secure physical destruction from a third-party hard drive destruction company using a chain of custody with verification of destruction.

2. Hard drives:
   a. Loose hard drives will be installed in a donor computer, and the above computer procedure followed to delete data on hard drive(s). FPOCF may also have the hard drives destroyed by a third-party company using a chain of custody with verification of destruction.

3. Flash media and Optical Media:
   a. Flash media files will be deleted. Deleted files on flash media are not recoverable
   b. Optical media will be physically destroyed by shredding.

4. Removable Media: Print Reports, CDs, Floppy Disks and any other storage media will not be discarded in the office trash or left in an unsecured manner as this would allow unauthorized access to the data.
   a. Confidential, HIPAA, and PHI data in printed form will be shredded.

b. Floppy Disks CDs and any other physical storage media will be made unreadable by physical destruction.

5. Storage:
   a. All devices awaiting data destruction shall be stored in secured areas until such time as the appropriate procedure outlined above can be performed.

6. Copiers:
   a. All copiers that are turned in to the leasing company will have their hard drive erased securely by either the leasing company and/or in concert with FPOCF.

All FPOCF computer users must return any data storage media upon employment separation or in the event the media is no longer required. This should be turned into the MIS Director of designee for proper data destruction. All such returned media must be signed by the FPOCF IT staff member on the transfer/disposal form indicating receipt of the returned item. This is forwarded to those individuals with the required signature authority and will be given to the MIS Director or designee to update the asset inventory. NOTE: If an employee returns media or other company property and does not ensure a transfer form is completed, they may be held accountable for the item upon their departure from the agency. Failure to comply with this procedure should be reported as outlined in FPOCF procedure IT-803, Security Incident Reporting, and Tracking.

BY DIRECTION OF THE PRESIDENT AND
CHIEF EXECUTIVE OFFICER:

PHILIP J. SCARPELLI
President and Chief Executive Officer
Family Partnerships of Central Florida

APPROVAL DATE: 11/25/2025