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

PROCEDURE

Series:	**Information Technology**	**COA: RPM 5, 5.01, 5.02** **CFOP: 50-2, 50-04** **DCF Contract GJ401**

Procedure Name:	Removable Media/Software Use & Management
Procedure Number:	IT-802
Reviewed Date:	4/27/16, 4/16/24, 10/2/25
Revision #/Date:	11/12/2020 Replaces Existing IT-802 & IT-815
Effective Date:	12/12/08 (Removable Media Use & Management & 4/2/13 (Software Installation)
Applicable to:	Family Partnerships of Central Florida (FPOCF) staff and contracted providers.

Purpose: It is the procedure of Family Partnerships of Central Florida to define standards, and restrictions for end-users who have legitimate business requirements to use portable or removable media on any equipment connected to the FPOCF internal/external network(s), infrastructure, or related technology resources. This procedure also ensures compliance with the protocols and the Department of Children and Families requirements governing software installation and deployment, including license requirements, copyright information, and authorized software on FPOCF computer systems and network.

Definitions: **Removable Media (RM) –** is considered, but is not limited to, all devices and accompanying media that meet the following classifications:

- Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives.
- Memory cards in SD, Compact Flash, Memory Stick or any related flash-based supplemental storage media.
- USB card readers that allow connectivity to a PC.
- Portable devices with internal flash or hard drive-based memory that support mass data storage.
- Smart phones with internal flash or hard drive-based memory that support mass data storage.
- Digital cameras with internal or external memory support are being used as mass storage devices. (Digital cameras, if employed, are to be used for pictures ONLY.)
- Removable optical media, such as writable and rewritable DVDs and CDs.
- Removable magnetic media, such as portable hard drives.
- Any hardware that provides connectivity through wireless means such as (Wi-Fi, WiMAX, IrDA, Bluetooth, etc.
- Wired network access through USB, Category 5+, serial, modem, etc.
- Any hardware and related software that could be used to access corporate resources.

Range of Threats When Using Removable Media

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive Covered Data, Confidential data, or proprietary information is deliberately stolen and sold by an employee.
Copyright	Software copied onto portable memory device could violate licensing.
Spyware	Spyware or tracking code enters the network via memory media.
Malware	Viruses, Trojans, Worms, and other threats could be introduced via external media.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the agency to the risk of non-compliance with various entities.

Proprietary Software - also known as non-free software, or closed-source software, is computer software for which the software's publisher or another person retains intellectual property rights—usually copyright of the source code, but sometimes patent rights.

Copyright - The right granted by law to an author, publisher, or distributor, for exclusive production, sale, or distribution of specific computer software or a computer software package.

Authorized Software – Computer software approved by Information Technology as a department standard.

References: GOV-202 Internal Controls, GOV-203 Risk Management, RQ-504 Records Retention Destruction

Procedure: In order to properly and reasonably secure and protect company and client information and ensure compliance with protocols and DCF requirements governing software installation and deployment, including license requirements, copywritten information, and authorized software on FPOCF computer systems and network, the following procedures will be enforced to all end-users of FPOCF personnel and Independent Contractors & hosted guests.

A. Security Responsibilities:

Securing access to and ensuring availability of agency data is the responsibility of the FPOCF Information Technology Department (IT) under the management of the MIS Director.

Securing access to state systems and databases used in the performance of operations is the responsibility of the Data Security Manager under the management of the MIS Director.

All FPOCF staff, providers, and others with access to agency documents, and the network have the responsibility to act in accordance with all agency policies and procedures. Data and information should always be stored and accessed on the network servers. This ensures data

security and integrity of the organization's information. No data should be stored on the computer's hard drive or on RM.

B. Authorized Users of Removable Media:

Access to RM for staff will be based on the need to perform duties apart from the conventional storage infrastructure. Requests for these are authorized by the division leaders and submitted to the MIS Director for final approval. All such requests will be submitted with a user access form, and a new inventory equipment form will be completed as well.

Independent Contractors and Conference Presenters:

Where it is necessary for an Independent Contractor to bring data into the FPOCF network for reasons such as presentation, training, or other such requirements, if the media is to be used on an agency computer, the media must first be scanned by the IT department. This ensures no risk of introducing any malware or virus to the FPOCF network. If the RM is connected to the guest's computer and that computer is only connected to the video presentation equipment and not connected to the network, then this would be considered acceptable. In these instances, IT should be contacted in advance to provide guidance or assistance to minimize the potential risk to the FPOCF network.

C. Use of Removable Media:

It is the responsibility of any staff, independent contractor or others who are requesting the connection of RM to the organizational network to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. Approval must be authorized before any RM can be connected. Accordingly, the following network rules will be observed:

- IT will limit, by physical and non-physical means, the ability to connect RM to the agency's network infrastructure.

- All RM is made available to staff and approved provider staff must be supplied and managed by IT. In managing the RM, IT will document the chain of custody to include the staff member, other individual acting as custodian of the RM and the intended use of the device. Authorized users will sign the RM and date of intended return. The supervisor will initiate a User Access form with appropriate signatures authorizing the issuance of the RM to an individual, and the individual will also execute the transfer form.

    - IT will assign and record the original password to the device. Users are not to change the password in order to allow IT to support and or recover data stored (IT CANNOT recover data from any RM without the original assigned password).
    - Users are not allowed to share their password with the device.

- All authorized users of RM will physically secure all such devices used for this activity whether they are actually in use and/or being carried. Reasonable physical security will include but not be limited to keeping the device out of plain sight, carrying the device on

or near one's person, locking the vehicle if the device is in the vehicle, office, or home where the device is stored or transported, etc.

- All RM will contain an encrypted area requiring a password to open, except as otherwise noted. All data stored on the RM will be contained in this area. The President and CEO may have a RM with a non-encrypted area. However, no client confidential or Covered Data is allowed to be placed on the non-encrypted RM.

- All agency staff, independent contractors, or others will not make modifications of any kind to company-owned and installed hardware or software and will not bypass encryption measures. This includes but is not limited to reconfiguration of USB ports, installation of CD/DVD burning devices, other data management software, or non-use of the encrypted area.

- FPOCF, IT restricts the use of Universal Plug and Play on its company-owned PCs. Those staff that require USB functionality will have to justify why they need access.

- The President and CEO may summarily ban the use of all RMs at any time (emergency provision). Protection of confidential and Covered Data is the highest priority.

- IT may limit the ability of authorized users to transfer data to and from specific RM on the network according to their specified needs.

- IT will keep an inventory of all RM. IT will check the RM periodically to ensure it is still in the possession of the authorized users to which it was issued and is still being used for the purpose intended. A user can retain the RM for any period of time as is appropriate and required. IT may at this time inspect the device to ensure all data is stored in the encrypted area.

- Authorized users and/or their supervisors must inform IT of any change in a user's role which would require the device(s) issued to be returned. This includes but is not limited to a change in position, a change in duties, or termination. A User Access form will be completed on the individual when a change in RM is approved.

- The authorized user agrees to immediately report to his/her manager and to IT any incident or suspected incidents of unauthorized data access, data loss and/or disclosure of agency resources, databases, networks, etc. This would include loss, theft (for which a police report should be filed), or any other circumstance in which agency data or property may have been compromised. FPOCF Security Incident Reporting procedures should be followed.

- Upon return of an RM to be made available for redistribution, IT will perform a complete scrub of all data on the RM and prepare the media for the next user. If the RM is no longer usable, the device will be physically destroyed as outlined in procedure RQ-504, Records Retention and Destruction.

- No individual is permitted to use a personal RM to connect to the FPOCF network at any time.

D. Software Installation:

- FPOCF's IT Department is exclusively responsible for installing and supporting all software on the FPOCF computers.

- Agency staff and those volunteers, independent contractors, interns, temporary staff or board members of their respective agencies, and sub-contractors are not authorized to install software of any type without the express approval and/or assistance of FPOCF IT Department. An upgrade to existing software is performed by the FPOCF IT department, and users are not permitted to do so.

- Software falling into one or more of the following categories are not allowed on FPOCF computers:

    - A piece of software purchased for one's home computer;
    - A downloaded software product, add-on, or component from the Internet;
    - Non-Agency Remote Access software such as GoToMyPC or LogMeIn; and
    - Illegal, unlicensed, or pirated copies of any kind.

- Only computer software documented as authorized software may be used on any computer owned by FPOCF or used to connect to the FPOCF network.

- Copyright statutes do not preclude the imposition of liability for copyright infringement on governmental agencies or their staff. According to Title 17, United States Code, section 101 et seq., the federal copyright act protects the interest of persons who have developed original works of authorship, including computer software. Illegal reproduction of software can be subject to civil damages and criminal penalties, including fines and imprisonment.

Failure to comply with this procedure, in the sole discretion of the agency, may result in the suspension of any or all technology use and connectivity privileges, disciplinary action up to and including termination; or, in the case of a contractual relationship, termination of the Agreement or Contract.

Upon learning of any failure to comply with this procedure, IT shall report the finding to the Director of MIS who will coordinate with the appropriate FPOCF Chief Administrative Officer to immediately report the situation. Based on the infraction, the situation may be addressed by the Risk Committee and/or the Executive Team. In all cases the Director of MIS will inform the President and CEO of each situation as it is surfaced.

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

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