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

PROCEDURE

Series:	**Information Technology**	**COA: RPM 5.01, 5.03, PRG 4.01** **CFOP: 50.2** **DCF Contract: GJ401**

Procedure Name:	Information Technology Network Monitoring
Procedure Number:	IT-804
Revision #/Date:	6/1/09, 3/18/13, 4/27/16, 10/8/2020, 10/2/25
Reviewed Date:	4/16/24
Effective Date:	12/12/08
Applicable to:	All Users of the Family Partnerships of Central Florida (FPOCF) Network

PURPOSE: It is the procedure of Family Partnerships of Central Florida to routinely monitor the technology infrastructure through which data and information are managed and shared. The methods ensure accuracy, integrity, and reliability, timeliness, and security and confidentiality of data and information. The monitoring of our network activity will help ensure that only authorized individuals access company or client data.

Definitions: **FPOCF Network –** A system containing any combination of computers, computer terminals, printers, audio or visual display devices, removable media devices or telephones interconnected by telecommunication equipment or cables: used to transmit or receive information.

Network Administrator (NA) – The person assigned to act as the Network Administrator for FPOCF.

Active Directory (AD) - Is a directory service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.

References: GOV-202 Internal Controls, GOV-203 Risk Management, IT-806 Accounting System User Rights Maintenance

Procedure: In order to properly and reasonably secure and protect company and client Information, the following monitoring procedure will be followed:

FPOCF will monitor and review the following reports/logs as indicated.

A. Monitoring Protocols Daily:

- Windows Azure Active Directory (AAD) recently created users.

- Monitor AD for possible unauthorized user threats. If there is no activity, no report will be generated. There will be no action by the NA.

- Windows Azure Active Directory (AAD) recently added computers.

  - Monitors AD for unauthorized access to physical networks. If there is no activity, no report will be generated. There will be no action by the NA.

B. Monitoring Protocols Weekly:

- Backup Logs
  - Monitor for successful completion of backups. Any failed backups will be documented along with corrective actions taken.

- Windows Azure Active Directory (AAD) recently modified users.
  - The NA will also monitor any unauthorized "access" to the FPOCF network which may include "authorized" users but who attempt to connect to the FPOCF network utilizing "personal" computing equipment of any type. In this rare instance, the NA will identify the equipment and alert the MIS Director. The "user" and/or equipment will be identified and kept from accessing the system again.

  - Monthly system uptime report is generated weekly regarding the servers to identify outages, and/or issues that need to be corrected.

To manage the network environment in the most efficient and safe manner possible, including the protections addressed above, at **NO TIME** are privately owned computers, flash drives or other removable media devices permitted to connect to the FPOCF network. Any exception to this must be authorized in advance by submitting a ticket to the helpdesk. The NA will consult and discuss the security risks with the MIS Director before the device can gain access to the network.

C. Monitoring Protocols Monthly:

- Windows Azure Active Directory (AAD) users never logged on.
- Monitors user accounts created but that have never been used. In this rare instance, the account is deleted.
- Windows Azure Active Directory (AAD) real last login.
-
  - Monitors the last time users accessed the network.
  - Monitoring should identify users who have not logged in for a period of 30 consecutive business days.
  - Monitoring may also identify users who have logged in at a very odd time (possible social engineering intrusion).

D. Monitoring Protocols as Needed and Upon Incident:

- APC Power Chute for the incident location.
  - Monitors a power event and provides detailed information to help maintain uptime during future power events.

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

Reporting Security Violations

Any security violations or incidents, related to network systems, computer equipment or identified in any monitoring report will be reported in accordance with internal Operating Procedures and CFOP guidance.

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