

---

<b>Series:</b>	<b>Information Technology</b>	<b>COA: RPM 5, 6.01, 6.03, 8.01, 8.02 CFOP: CFR45, CFR 164.308(a)(1)(ii)(d)</b>
<b>Policy Name:</b>	<b>IT Network Monitoring</b>	
<b>Policy Number:</b>	<b>IT-804</b>	
<b>Revision #/Date:</b>	<b>(3) / 6/07/10</b>	
<b>Effective Date:</b>	<b>12/12/08</b>	
<b>Applicable to:</b>	<b>All BFP IT Staff</b>	

---

SUBJECT: IT Network Monitoring

PURPOSE: The purpose of this procedure is to define daily, weekly and monthly reporting of BFP network activity to help assure only authorized individuals access company or client data.

POLICY:

### References

BFP Policies/Procedures: GOV-202, GOV-203, IT-806

### Definitions

BFP Network: a system containing any combination of computers, computer terminals, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment or cables: used to transmit or receive information.

### Monitoring Protocols

In order to properly and reasonably secure and protect company and client information, the following monitoring will occur:

- The following reports will be monitored **daily**:
  - Windows Active Directory (AD) Recently Created Users
    - Monitors AD for possible unauthorized user threats. If there is no activity, no report will be generated. This fact will be noted by the Network Administrator.
  - Windows Active Directory Recently Added Computers
    - Monitors AD for unauthorized access to physical network. If there is no activity, no report will be generated. This fact will be noted by the Network Administrator.

- The following reports will be monitored **weekly**:
  - Backup Exec Tape Backup Logs
    - Monitors tape backups for bad tapes, bad drives, and successful backups.
  - Windows Active Directory Recently Modified Users
    - Monitors AD for unauthorized self promoted internal user threats.
  - Microsoft Exchange 2007 User Hidden
    - Identifies users whose active directory account has been disabled (they've left BFP) and their email account is still active (mail needs to be disposed of appropriately).
- The following reports will be monitored **monthly**:
  - Windows Active Directory Users Never Logged On
    - Monitors users created who have never used their account and, subsequently, should be deleted.
  - Windows Active Directory Real Last Login
    - Monitors the last time users accessed the network.
    - Monitoring should identify users who have not logged in for a long time (need deletion).
    - Monitoring should identify users who have logged in at very odd times (possible social engineering intrusion).
  - Microsoft Dynamics SL aka 'Solomon' User Group and User Record Reports
    - These reports identify which user groups or individual user access has been changed during the time period selected to monitor.
    - These reports will be produced for each calendar month to capture all changes. These reports will then be reconciled with the corresponding Solomon User Rights Forms to verify accuracy and to assure appropriate approval for changes recorded. Reference procedure IT806 – Accounting System User Rights Maintenance for further details.
    - These report reviews and subsequent reconciliations will be performed by the Financial Analyst or, in their absence, a designee appointed by the Chief Financial Officer (CFO).
- The following reports will be reviewed at a minimum **annually**:
  - Microsoft Dynamics SL aka 'Solomon' Access Rights
    - Identifies which groups are assigned specific access rights.
    - Identifies which users are in which groups.
    - This report review will be performed by the Financial Analyst or, in their absence, a designee appointed by the CFO.
- The following reports will be reviewed **upon incident**:
  - APC Powerchute for the Incident Location

- Monitors a power event and provides information to help maintain uptime during future power events.

All monitoring reports listed, excluding the Microsoft Dynamics SL, will be reviewed by the Network Administrator to identify any anomalies which may indicate or lead to a data security issue or data loss.

Microsoft Dynamics SL aka 'Solomon' Access Rights Report will be managed as outlined in BFP procedure IT-806, Solomon Accounting System User Rights Maintenance.

### **Processing an Identified Monitoring Anomaly**

For all monitoring reports listed, excluding the Microsoft Dynamics SL, upon identifying an anomaly, the Network Administrator will create an IT work order defining the anomaly. If the anomaly does not pertain to an IT staff member, the Network Administrator may delegate the research of the event to the IT staff. Otherwise, the Network Administrator will investigate the anomaly. The results of such research will be noted on the IT work order. The anomaly may be corrected as appropriate and the steps taken to correct it must be notated on the work order. If the anomaly appears to be systemic, the work order will be escalated and reported to the CFO.

Anomalies identified in the Microsoft Dynamics SL aka 'Solomon' User Group or User Record Reports will be investigated by the CFO. Documentation of the anomaly and correction will be made in memo format. Any internal control violations will be communicated to the Chief Executive Officer (CEO) and further action if necessary.

### **Reporting Security Violations**

Any security violations or incidents, as defined in BFP procedure OP-1050-19: Security Incident Reporting and Tracking, identified in **any** monitoring report will be reported as outlined in the before mentioned procedure.

BY DIRECTION OF THE CHIEF EXECUTIVE  
OFFICER:



DR. PATRICIA NELLIÜS-GUTHRIE  
Chief Executive Officer  
Brevard Family Partnership

APPROVAL DATE: 6-3-10