DISASTER RECOVERY PROCEDURES

(Effective 2004)

Revised Date:

12/20/11
08/20/12
09/10/13
01/12/14
03/15/15
04/25/17

THE RESOURCE CENTERS

4360 Northlake Blvd Ste 206 Palm Beach Gardens, FL 33410 ❖ Ph: (800) 206-0116 ❖ Fax: (561) 624-3278

Should circumstances demand activation of a business recovery plan to insure continuation of all essential operations, the Resource Centers will implement and follow the procedures contained herein. The Disaster Recovery Procedure, last updated September, 2013, is incorporated in its entirety into the polices and operating procedures for the Resource Centers LLC and affiliated companies.

Primary Notification

Upon activation of the Disaster Recovery Plan, the following information will be immediately provided to the team leader(s):

1. Nature and location of disaster:

   _____

2. Name of Emergency Management Team Coordinator:

   _____

   Location:

   _____

   Phone number, fax number, and Email contact for Command Center:

   _____

3. Backup location:

   _____

4. Telephone number for staff to call for status updates:

   _____

5. Special instructions or considerations:

   _____

   _____

   _____

   _____

   _____

   _____

Procedures

Notify Team Members & Determine Status of All Affected Personnel

This manual includes lists to contact every employee of the company.

Appendix A contains the Call List/ Team List, which shows the entire organization in a "call tree". The call tree identifies the person responsible for calling other team members. The calling sequence can be implemented at any point along the tree, in the event that a person is not available.

Appendix B contains the core recovery team list. The designated Emergency Management Team Coordinator will contact this team to implement the business recovery plan. The following items will be addressed:

1. Review the situation.

2. Determine if and where key personnel can meet to review plans in detail.

3. Using the team list, identify the additional members of the organization who will be called in to implement the business recover plan.

4. Using the team list, identify the personnel who will maintain essential operations and perform time critical tasks.

5. Using the team list, update the remaining staff regarding the situation. Staff will be notified of any temporary location for operations and any new contact information. The Emergency Management Team Coordinator will notify staff when they might be called to report to work.

Initiate Recovery Progress Logs

Appendix C contains a template for the Recovery Progress Log; however, any note pad will do. The daily log will include the following information:

1. Date.

2. Time.

3. Description of all tasks and processes implemented, with relevant comments.

4. Names and contact information for emergency managers, clients, or other persons assisting with recovery efforts.

5. Initials of the person making the entry (if multiple people use the same log).

The log must document all major activities that occur. This information may be essential to continued recovery efforts, in addition to post recovery evaluation of the business recovery plan. Furthermore, the information will also be required for insurance and legal purposes. The Emergency Management Team Coordinator or designee shall take responsibility to enter information in a formal recovery actions log and transfer informal notes compiled by team members. The Coordinator will continue to update and maintain the log throughout the recovery process and during the return to a primary facility or base of ongoing operations.

Review Recovery Priorities

Each business function has been assigned a priority level (high, medium, low) and a recovery sequence:

Function	Priority Level	Recovery Sequence	Required Equipment
Recordkeeping Services	High	1	Server
Member Distributions	High	2	Server, 4050 Printer, Mikr Toner, Check Stock
Cash Movement	High	3	Workstation/ Internet Access and/ or Fax
Communication with Clients	High	4	Workstation/ Internet/ Phone/ Fax
Preparation for Meetings	Medium	5	Server
Compliance, Research Inquiries	Medium	6	Server
Client Service Calls	Low	7	Server
Presentation Preparation	Low	8	Workstation
Response to RFPs	Low	9	Workstation

Perimeter Network Server Cluster

Server	Description
Database Server DBServer	Database
Email Server EmailSRV	SMTP/POP3 Server, File Server
File Server FileSrv	DC, File Server, Printer Server, Backup Storage
Development Server DevelopSrv	Web Server, File Server

Network Description

The Primary Network Server Cluster supports the following core functions: the Network Domain Controller; Data Servers; Exchange Server for local and global E-mail functions; primary Cash Management and defined benefit pension recordkeeping systems; software applications and data files; and the on-site and off-site daily systems and data backups. Each server that supports mission critical functions includes a fully operational mirror server in case of the failure of any single component.

The Perimeter Network Server Cluster supports the Internet and web applications, FTP site for external transfer of data, and the ISA high security Firewall Server. These servers also include a fully operational backup server in case of the failure of any single component. The ISA Server provides an external security layer and an internal security layer to separate applications that allow external access of systems by Internet clients from the Primary Network Server Cluster. This security layer that separates the Perimeter Network Server Cluster from the Primary Network Server Cluster safeguards sensitive systems and data from external intrusion.

External access is controlled through redundant high-speed Internet connections to insure continuous access in the event of a service failure by an external service provider. External Clients access the Perimeter Network Server Cluster through an encrypted Secure Socket Layer (SSL) connection. Both Adelphia (Comcast) and BellSouth provide high-speed Internet connections to the Perimeter Network Server Cluster. Each company provides Internet access to a static IP address. In the event of a service failure by either company, Internet access must be redirected to the backup IP address through the Network Solutions control panel.

At a minimum, a single server and either Tera Station can support all operations from an alternate location with high-speed Internet access in a catastrophe.

Implementation Plan

Call Personnel for High Impact (Essential) Operations

Using the call list, the Coordinator will notify the individuals required to perform essential functions. These individuals should be advised where to report, along with any additional information that they will need to begin work. The Coordinator should also communicate such information as the hours the person will be expected to work, living arrangements if the person will be required to relocate, and the availability of amenities (items like restaurants, break rooms, restrooms, etc.)

Depending on the circumstances, team members may need to travel to another location requiring overnight or extended stays.

Notify Entire Staff

Not all staff members may be required to implement the business recovery plan or provide immediate services, but these staff may be considered alternate or "relief" personnel. In some cases, the situation may already involve the entire staff. Anyone not required to immediately report should at least be called and updated on the situation, with an expected time frame to either report or resume normal operations.

Refer Media Contacts to Management

Ensure that personnel refer all media contacts to the Emergency Management Team Coordinator or other management designee.

Verify Availability of Resources

If the situation does not require operations to move to another facility/ location, then each affected area of operations must be assessed to determine the resources available on site, determine which resources are not available, and identify any unexpected needs.

The team members should review the following categories of resources in order to compile a detailed inventory of assets, as well as equipment requiring repair or replacement:

- Availability of Power
- Hardware/ Software
  - Servers
  - Network Switch & Router
  - Network Cables/ Communication
  - Workstations
  - Printers
- Telecommunications
  - Phone
  - Fax
  - Internet
- Office Space

- Condition/ Availability of Furniture
- Critical Records
- Forms & Supplies

Items requiring repair or replacement should then be ranked according to the most important business functions identified in the recovery sequence.

Relocate Essential Documents to Alternate Facility

If operations must be provided from an alternate location, the following documentation should be available at that location:

1. Plan Documents/ Current Information
2. Client Contact Information
3. Legal Files and Contracts
4. Forms and Supplies

Notify Support Services

The following support services must be notified of changes:

1. Mail should be temporarily held or routed to the new location.
2. Incoming phone numbers should be reactivated/ switched to the new location.
3. Temporary and permanent connections for Internet and Email service should be established.
4. Courier services, if needed, should be arranged.

Initiate Recovery of Servers

The server incorporates the following safeguards:

1. The data servers write all data files simultaneously to a hard drive array.
2. Each server runs on a battery backup with redundant power supplies. Each mission critical server has a secondary backup server that mirrors the primary server.
3. All programs and data backup daily to two separate backup units, one on-site and one off-site. Each Tera Station data backup contains the files and data to run all critical functions when connected to a server.
4. At least one workstation contains current duplicates of all server functions and data. This laptop can function as a surrogate server at any location, or the laptop can run all essential functions as a standalone computer.

The following applications and data locations should be verified following reactivation of the server:

1. Defined Pension Benefit Systems on shared data Drive F.

   These directories must all reside on the same network drive:

Benrec	Pension Payment and Cash Management Systems
Penben	Defined Benefit Recordkeeping Systems
Letter	Benefit Letter Extracts
Upload	ACH Files & Check Recon Files
Spool	Spooled Reports

   Check factory can reside on any network drive:

Cfactory	Check factory– LFEWIN2.EXE

   The following environment variables must be set on each workstation:
   SET COBSW = +C +C4
   aslmfnet = f:\mfaslmf

2. Macola (Accounting System) on shared data Drive M.

3. Common data files on shared data Drive S.

4. Microsoft Outlook for Email access.

5. Microsoft Exchange Server for office communications.

6. Internet access or connection.

Coordinate Vendor and Service Support

Coordination with vendors will be necessary to acquire resources or services not provided through the Resource Centers. Appendix D lists facility management contacts and phone numbers, phone numbers for telecommunication and Internet service providers, banking information, and contact/ phone numbers for additional computer systems support.

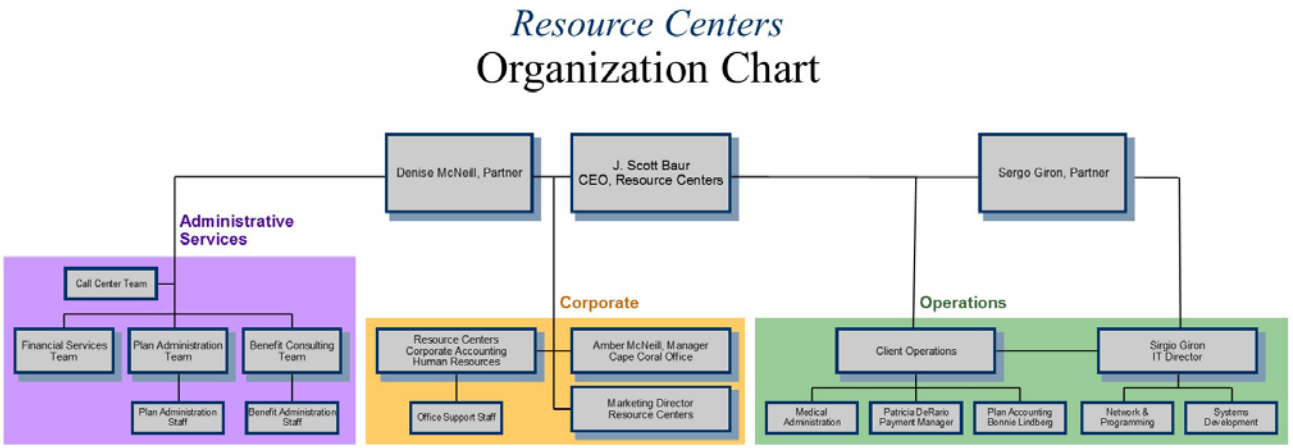
Notify Key Client Contacts

Appendix E contains contact sheets, with additional contact information for third party service providers, for all client groups. These individuals should be notified as soon as possible regarding the details for continuing account service during the disaster recovery period, including new office contact information, address if necessary, and anticipated time frame until full restoration of normal operations. The Resource Centers will update key contacts on recovery progress until normal operations are resumed.

Appendix A: Call List

(Note: This page contains personal data and contact information for employees. Personal information was intentionally omitted.)

Organizational Chart



Appendix B: Core Recovery Team

Team members may change depending on the location or nature of the disaster. The following chart details the composition for the standard recovery team: