# DISASTER RECOVERY PROCEDURES

LinkActiv will develop customized Disaster Recovery Plan as per specific client needs and requirements.

**Overview**

**<u>The LINKACTIV DRP address three main functional areas</u>**

**Recovery:**

Once the infrastructure is back in place it will be necessary to recover production data. Since recovery may not be up to the point of failure, it is important to identify any processing that needs to be redone. Can all of the data feeds to the system be identified? How many of them can be redone with 100% certainty of success? It is important to minimize "holes" in data (especially in a distributed processing environment where one step could be dependent on one or more predecessor steps or actions), and then to identify the action to be taken when data inconsistencies are detected. There should be an audit trail for all work performed during this phase. Once the data is recovered there should be some type of validation process (discussed in more detail below) to ensure that the recovery was complete, leaving a consistent work environment.

**Restoring / Sustaining Business Operations:**

Critical business processing (which may not encompass all application systems) will need to be supported. All processing requirements and service level agreements need to be defined and documented. Dependencies between processes also need to be defined. It is important to document the existing process and then build the plan accordingly. Anything that ran before (in production) will probably need to run again (at the hot site), so scheduling and dependency information is critical. Remember that routine maintenance (including backups) should still be performed at the hot site (it too is an asset that requires protection).

**Transferring Data back to Production Servers:**

This is one area that is very important. A process needs to be defined to manage this migration. Often the best approach is to execute the DRP on the production servers in order to synchronize the systems to a specific point in time. It should also be noted that this is one of the more difficult tasks to test.

**<u>The LINKACTIV DRP address three main technical areas</u>**

**Hardware Issues:**

This includes equipment restoration, configuration (disk capacity, peripheral devices, device names, RAM, file systems and volume groups, 08 users, etc.) and operating system version and patch level.

Another issue is deciding whether to use an existing pre-configured machine template or to completely configure a machine (load the OS, initialize and configure disks, TCP/IP configuration, SCSI addresses, everything). There are pros and cons to each scenario. LINKACTIV IT Team approach must be to plan for the worst case (i.e., the complete rebuild). Note: It may be possible to reconstruct the production machine on a new machine using a tape backup. This method does not leave much room for flexibility relative to hardware configuration, but is very fast when compared to a manual system reconstruction.

The key to success is to ensure that DRP machines have at least as much capacity as the production machines that they are replacing, that they are compatible architectures, and that the "designee personnel" has the installation media for the 08 load.

**Networking Issues:**

What part of the production system must be replicated for the DRP? This environment most likely consists of several machines, and there is a good chance that the environment is not suitable for a total replication. IT Team must try to avoid scenarios where the applications connect to machines using hard-coded IP Addresses rather than hostnames (which is preferable) what other configuration information is required? Are there requirements for connections to an external network (WAN, Internet, Extranet) documented and update? Is there any other type of Client/Server or n-tier activity that will need to be supported? All networking requirements and issues need to be identified, documented, and then addressed in the DRP.

**Software Issues:**

This is a very broad area that encompasses many things. Software includes the Operating System, user written applications, and third party software (RDBMS, report writers, GUI products, backup/recovery products, scheduling software, etc.). A comprehensive inventory of currently used software, including current version, license information, and support contact information is part of the DRP.

Whenever possible it is preferable to be using current versions of the products in production (for improved product support). It is also desirable to have the installation media, installation guide/notes, licensing information, support information, and current configuration information available for these products (all of which is critical for rebuilding the installation).

Regarding custom applications, it is desirable to have the source code, libraries, and "make" files in addition to the executable code. There is always the chance that the application will need to be recompiled due to version incompatibilities, bad executables, path changes, etc.

**Creating the Procedures that Support the DRP**

Execution of the plan will be stressful and people may forget simple, everyday things. Also, resources/staffing may change and the people assigned to execute the DRP may not be familiar with it. The use of the DRP session checklists is very desirable. These lists should have sections for a timestamp, initials of the person doing the work, and room for comments. This information will be critical if a problem is found downstream.

Despite the fact that the complete IT Team is part of the disaster recovery efforts a single person should be identified as a DR Coordinator (the IT Director), with a backup person identified to fill-in if necessary. The IT Director will be responsible for monitoring each phase of the DRP, coordinating with the various groups involved with executing the DRP, and providing status information to the Management of LINKACTIV during DRP execution. Resources should be identified within each department or LINKACTIV functional area as being responsible for each and every task and procedure, and they should know exactly what is expected of them. Again, nothing should be left to chance!

Data should be gathered during testing (e.g., reports, screen prints, transaction logs, etc.) and saved for future review. In the event of problems that data may help the team make a root cause determination regarding the problems that it can be corrected. If everything goes right it provides the necessary documentation to support an external validation effort of the DRP exercise. The only way to really know if "everything worked" is to know what “everything" is, and then to be able to demonstrate that the necessary tasks were completed successfully!

Disaster Recovery Check List

1) Maintenance of the disaster recovery plan

- Establish a disaster-recovery team of employees who know your business best, and assign responsibilities for specific tasks.
- Identify your risks (kinds of disasters you're most likely to experience).
- Prioritize critical business functions and how quickly these must be recovered.
- Update and test the plan at least annually.

2) Alternative operational locations

- Determine which alternatives are available.
- For LINKACTIV the most suitable alternative is the APEX facilities

3) Validate status of the Backup site.

- Power generators.
- Computers and software.
    - Critical computer data files (payroll, accounts payable and receivable, customer orders, inventory).
- Phones/radios/TVs.
- Equipment and spare parts.
- Vehicles
- Digital cameras.
- Common supplies.
- Supplies unique to your business (order forms, contracts, etc.).
    - Basic first aid/sanitary supplies, potable water and food.

4) Safeguard the LINKACTIV property

- The building
- The equipment
- The computer systems
- The company and customer records
- Other company assets

5) Contact information

- Keep current and multiple contact information (e.g.,home and cell phone numbers, personal e-mail addresses) for: — Employees
- Key customers
- Important vendors, suppliers, business partners
    - Insurance companies

6) Communications

- LINKACTIV must have access to multiple and reliable methods of communicating with your employees:
- Emergency toll-free hotline - Yes
- Website - Yes
- Cell phones - Yes
- BlackBerry(TM) - Yes
- -Two-way radios - Yes
- Internet - Yes
- E-mail – Yes

7) Employee preparation

- Make sure LINKACTIV employees know:
- Company emergency plan.
- Where they should relocate to work.
- How to use and have access to reliable methods of communication, such as satellite/cell phones, e-mail, voice mail, Internet, text messages, BlackBerry(TM), PDAs.
- How they will be notified to return to work.
- Emergency company housing options available for them and their family.

8) Customer preparation

- Make sure LINKACTIV key customers know:
- Your emergency contact information for sales and service support (publish on your website).
- What to expect from your company in the event of a prolonged disaster displacement.

9) Evacuation order

When a mandatory evacuation is issued, be prepared to grab and leave with critical office records and equipment:

- Company business continuity / disaster recovery plan and checklist.
- Insurance policies and company contracts.
- Employee payroll and contact information.
- Desktop/laptop computers.
- Customer records, including orders in progress.
- Photographs/digital images of your business property.
- Post disaster contact information inside your business to alert emergency workers how to reach you.
- Secure your building and property.

10) Cash management

Be prepared to meet emergency cash-flow needs:

- Keep enough cash on hand to handle immediate needs.

- Use Internet banking services to monitor account activity, manage cash flow, and initiate wires, pay bills.
- Issue corporate cards to essential personnel to cover emergency business expenses.

11) Post-disaster recovery procedures

- Consider how your post-disaster business may differ from today.
- Plan whom you will want to contact and when.
- Assign specific tasks to responsible employees.
- Track progress and effectiveness.
- Document lessons learned and best practices.