



Disaster Recovery

Planning and Preparation

Definition

A disaster recovery plan describes how an organization is to deal with potential disasters. Just as a disaster is an event that makes the continuation of normal functions impossible, a disaster recovery plan consists of the precautions taken so that the effects of a disaster will be minimized and the organization will be able to either maintain or quickly resume mission-critical functions.

Developing a Disaster Recovery Plan

A disaster recovery plan describes what actions to take, when to take them, and how to complete the assigned tasks. It should be detailed and instructive and address the specific needs of every office of city or county government. The plan should anticipate the various types of disasters your city or county might face. A response to a flood will be different from response to a fire or earthquake or tornado.

A copy of the plan should be in a secure area within the office as well as at a secure, off-site location. The best recovery plan will do no good if the only copy is locked inside a file cabinet in an office that is burning down. A good suggestion would be to store a digital version of the plan on a server far away from the office site. The plan can be imported into Google Docs or other web based storage. It could also be emailed to a web based email account such as Hotmail, Yahoo, or Gmail.

A good disaster recovery plan will:

- Designate who is in charge of recovery operations and who will be working on recovery teams. It should include all necessary information for contacting these people at any hour of the day or night
- Anticipate the types of disaster the city/county may face and provide basic instructions for the first responders to an emergency to ensure that everything possible is done to minimize damage and preserve the safety of individuals responding to the disaster (e.g. evacuation plans, directions for shutting off electrical current in case of a flood, locations of shut-off valves in case of a broken water line)
- Include an inventory of supplies and equipment that are available for use in salvage efforts. The inventory should identify locations of important supplies and equipment—everything from heavy machinery to fire extinguishers to mops and buckets
- Identify alternative office space and other facilities which might be used if the city/county needs temporary space for relocation or salvage operations
- Include current contact information for experts in emergency management like TEMA, FEMA, and other governmental entities, plus commercial entities that can provide expertise in recovery and salvage if the disaster is too large for the city/county to handle by itself



- Have a plan for acquiring replacement office equipment and supplies quickly and efficiently. This will be especially essential if computer equipment was damaged in the disaster.

A good disaster recovery plan should include:

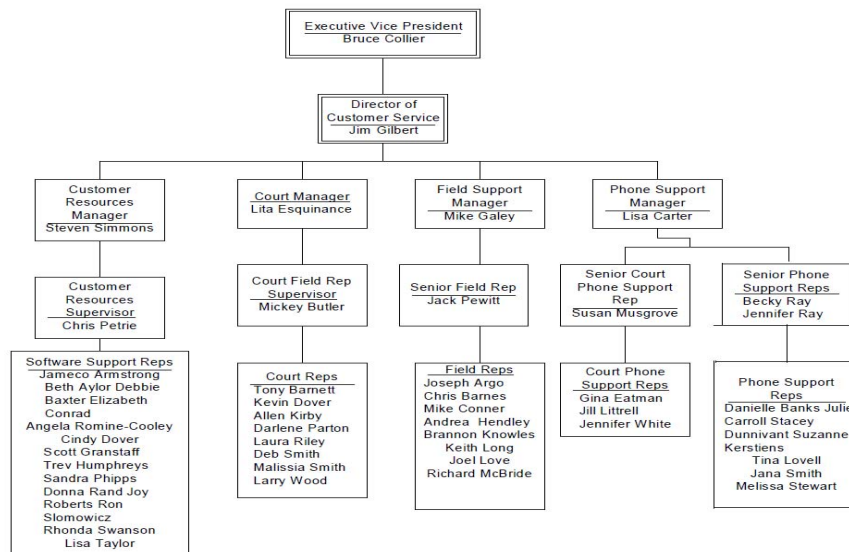
Organization Chart

Your organizational strategy is centered around the development and communication of your Organization Chart. The Organization Chart takes the form of a graphical representation of the positions in your organization. The top Position in the organization is placed at the top of the organization chart and the various layers of management and supporting positions are then arranged under the relevant management positions right down to the lowest levels.

Your organization chart not only defines the positions in your organization but the employees assigned to those positions. The organization chart clearly communicates the management and reporting structure of your organization, specifically who an employee assigned to a position reports to directly.

Develop the positions in your organization chart to be representative of specific work roles in your organization. You should not develop your organization chart based on the employees you currently have, rather you should develop the positions based on logical groupings of work. One of the benefits of developing an organization chart is that it enables your organization to become less dependent on specific employees and more dependent on the structure that you have developed.

Organization Chart Example:





Recovery Procedures

Strategic written recovery procedures should be developed, maintained and documented for all departments, offices, facilities, functions, and personnel

Strategic recovery procedures are designed to dedicate the institution's resources appropriately to:

- Minimize disruptions of services to the institution
- Minimize financial loss
- Ensure a timely resumption of operations in case of a disaster

Recovery procedures should create a strategic and tactical response based upon these priorities

- People: employees, customers and service providers
- Places: departments, offices and facilities
- Things: assets and records

Restoration Priorities

Your disaster recovery plan must not only spell out which functions are vital, but also the order they are restored. This is especially critical in accounting and computing functions where accounts receivable, payroll, and accounts payable have fluctuating priorities throughout the month.

Manual Processing Procedures

Documented manual processing procedures should be developed for users to perform business functions manually if the computer system is inoperable. This should include provisions to retain manually processed information for use when the computer system becomes operational.

Inventory

A written inventory should be maintained and included in the plan that includes the following:

- Hardware components
 - Servers
 - Workstations and laptops
 - Printers
 - Networking (routes, switches, etc.)
- Software components
 - Operating systems
 - Software applications
 - Software licenses
 - Release versions
 - Vendor names
- Communication components
 - Phones
 - Modems
 - Phone lines
 - Cabling



Documentation

Important documentation should be maintained and included in the plan. Copies of this documentation should be stored at a secure offsite facility. This documentation includes the following:

- User documentation
- Policies
- Procedures
- Manuals
- Contracts

Extra Stock of Paper Supplies

Extra paper supplies should be stored at an offsite location. These supplies should include:

- Paper
- Checks/Warrants
- Requisitions
- Purchase Orders
- Receipts
- Returns
- Bills/Invoices

Contingency Site

A contingency operation site should be designated in case a disaster makes normal functions at the current site impossible. There should be a signed contract for the use of the contingency site. Periodic evaluations of the contingency site's operating environment should be conducted to ensure that it is compatible with the current level of technology being used at your office.

Things to consider:

- Laser printing vs. dot matrix
- Laser paper vs. green bar paper
- Laser checks vs. dot matrix
- Other laser forms vs. dot matrix (receipts, forms, etc.)

Monitor/Modify the Plan

Once a disaster recovery plan has been established, it is critical to monitor the plan to ensure its components are implemented effectively. A disaster recovery plan should be viewed as a living, breathing document that can and should be updated frequently, as needed. Proactive ongoing monitoring and remediation of processes, such as backup data storage, results in fewer computer/software issues and less downtime should a crisis occur.

Test Disaster Recovery Plan

The ability of the disaster recovery plan to be effective in emergency situations can only be assessed if rigorous testing is carried out. Testing should be done one or more times per year in realistic conditions simulating circumstances that would be applicable in an actual emergency.



The testing phase of the plan must contain important verification activities to enable the plan to stand up to the most disruptive events. Failure to test your disaster recovery plan leaves your organization vulnerable to massive technology and business failures in the event of a disaster. An under-tested plan can often be more of a hindrance than having no plan at all.

Backups

Backups are the single most important aspect of any type of recovery.

- Computer system should be backed up on a daily basis.
- You should have written backup procedures documented and included in your disaster recovery plan.
- A backup log recording backup date and location should be maintained.
- Perform off-site data backup and storage
 - Any catastrophe that threatens to stifle a organization is likely to make access to on-site data backup impossible
 - In a catastrophic situation, there is no benefit to creating backups of valuable data if this information is not stored in an offsite location

Recommended Backup Strategy

9 tapes/DVD's/CD's labeled as follows:

- 4 Monday thru Thursday
- 2 System Even
- 2 System Odd
- 1 System Maintenance

Monday thru Thursday you should perform a Daily backup that will overwrite the previous Monday thru Thursday's tapes. This backup should be rotated offsite and the previous day's Daily Backup returned. The most recent Daily backup should be stored in a secure location offsite and far away enough from the main office in the event of fire or other natural disaster.

The System Backups should be performed using the 5 tapes/DVD's/CD's labeled System Even, System Odd, and System Maintenance as follows:

- On a Friday that is on an even date use one of the tapes/DVD's/CD's labeled System Even. Rotate this offsite. Bring back the previous System Even
- On a Friday that is on an odd date use one of the System Odd tapes/DVD's/CD's. Rotate this offsite. Bring back the previous System Odd
- Before performing monthly maintenance such as defrag and disk cleanup, you should backup using the System Maintenance media

At a minimum, store the most recent System Even and System Odd backups in a location OFFSITE and far away enough from the main office in the event of a disaster



Remember: If a disaster occurs that renders your computer system inoperable, the latest available backup is restored. Any work that was done between the time of the disaster and the time the latest back up was done will be lost!

Data Restoration Testing

Backups need to be checked daily to verify that the backup completed successfully and that there are no pending problems with the hardware. Automated backups are not recommended due to the difficulty in verifying backups complete successfully and being alerted to potential hardware issues. Regular test restorations need to be performed to validate that a restoration can be accomplished during a disaster.

Backup Workstations and Laptops

Users often store important files on local desktops and laptops. Backing up laptops and desktops protects this critical data in the event of a lost, stolen or damaged workstation. Ways to backup workstations and laptops include:

- Flash drives
- DVD's/CD's are another option. However, CD's have a fairly low capacity for storage
- Same off site recommendations apply to these backups

Remember: Disasters do not have to be big to be devastating. Little emergencies like a leaky roof or a burst water pipe can do tremendous damage.