CORPORATE REALTY

WHEN DISASTER STRIKES

A Guide to Emergency Planning, Disaster Recovery and Business Continuity

Is Your Organization Prepared?

Have you thought of how your organization would respond if a natural disaster interrupted your work? While it's not something we want to think about, natural forces are not selective in the organizations they impact. Without adequate planning, organizations can suffer losses that may have been lessened by proper preparation.

This brief handbook will explain the points every organization, small or large, needs to think about in order to prepare its own disaster recovery plan. By using this plan, should a disaster occur, your organization will be able to recover quickly and resume operations effectively. Each organization structure and circumstances are unique and this plan can be tailored to suit your needs.

In creating a disaster plan, don't be overwhelmed by the task. Work on it in sections and prioritize as time allows. The most difficult thing is getting started; the second most difficult task is keeping the plan current.

Remember, there are no cookie-cutter templates – one size does not fit all. However, there are common elements among all plans. This handbook will assist your organization in developing a plan to ***Prepare***, ***Respond***, and ***Recover***.

What is a Disaster Recovery Plan and Why Should You Have One?

A disaster recovery plan is a user's guide for how to preserve an organization in the event of an interruption. In order for it to be useful, it must be created before the interruption occurs. The interruption can be as simple as a computer crashing or as devastating as a Hurricane Katrina. The goal is the same – to preserve the organization.

CORPORATE REALTY

For further information, please contact:

Maureen Clary, CPM
mclary@corp-realty.com
201 St. Charles Avenue, Suite 4411
New Orleans, LA 70170
504-581-5005 • 504-585-2605 (fax)
www.corp-realty.com

CORPORATE REALTY

There are three critical components to a Disaster Recovery Plan:

1. *Emergency Planning* – developing a plan to respond to a disaster or interruption in service
2. *Disaster Recovery* – steps taken to restore functions so that some level of service can be offered
3. *Business Continuity* – completing the process of getting your organization back to where it was before the interruption.

Part of writing a disaster plan is to think ahead to the possibilities of what could go wrong and make contingency plans. However, you cannot plan for every scenario. The goal is not to create a separate plan for a tornado, a flood or a blackout but to create a plan that will address a majority of the risks.

To begin, ask the following questions:

- What are the potential identifiable disasters?
- How would each affect the organizations systems and programs?

Factors to consider include:

- Historical: What types of emergencies have occurred in the community? (for example, hurricane, flood, utility outages, etc.)
- Geographical: What can happen as a result of our location? (transportation routes, power plants, etc.)
- Human Error: What emergencies can be caused by employees? Do they know what to do in an emergency?
- Physical: Consider what could happen as a result to the location of your facility. (i.e. access to your office, loss of power, water damage, structural damage, building collapse, etc.

Ultimately, there are several potential scenarios to plan for, regardless of the interruption or catastrophe:

1. Only your local office is unusable. For example, one or more offices become temporarily unusable because of flooding or minor damage.
2. The entire building is gone.
3. A temporary disruption of services, such as an electricity outage.
4. An impact in the larger geographical area, rendering the area uninhabitable for an unknown amount of time.

Assign a Team – You Can't Create a Plan Alone

It is important to assign the right team to help create your disaster recovery plan. Depending on the size of the organization, the team should include representatives of the various departments to provide needed input. Departments could include personnel, computer and technical support, and finance, board of directors, and facilities management.

For the plan to be successful, the team must have the authority to make short-term emergency decisions. There must be a chain of command. This chain should include those in leadership but not necessarily senior leadership. The members of the Emergency Management plan should be those fully familiar with the disaster recovery plan and available to implement the plan in the event of an emergency.

The team must be able to implement the plan in a logical and orderly fashion based on the nature of the organization and its services, as well as the type of disaster or interruption. This should all be addressed during the planning stages.

Remember, the organization must be able to implement the plan even if the person or team who created the plan is not available.

It has to be legible and understandable. Common sense must rule. The plan must be tested and employees must be trained on plan implementation. As the organization changes, the plan must be updated to reflect those changes.

Analyze your Organization

To begin to develop your disaster recovery plan, an organization must first determine their critical services and functions. The following questions can help you begin:

1. What are your organizations services and functions? (i.e. What do you do?)
2. What staff is responsible for what functions?
3. Which functions are critical and which are less so?
4. Whom do you serve? (who are your clients, what are their needs, etc.)
5. Where do you serve them? (on site, at their office, etc.)
6. How do you serve them? (what do you provide: information, research, advice?)
7. How are the services provided? (via phone, internet, in person?)
8. What are your personnel requirements? (are services provided by staff, contractors, etc?)
9. What are your equipment requirements?
10. How do you services impact the organizations functioning? (For example, if fee for services is crucial, what will happen if you cannot perform those services)

In order to have a contingency plan, differentiate your organization's services. If, for example, a phone system is critical, should you invest in having phone service with multiple providers? If it's your computer or website, this may be where you want to focus your resources. If you service depends upon on site visits, should you make arrangements with another organization to set up temporary office?

Make the Plan Step-by-Step

Step 1: Human Resources

For all organizations, people are the most valuable assets. It is important to protect your employees and have lines of communication before during and after a disaster. Areas to consider are:

- Include disaster planning and preparation as part of your employee policies
- Keep updated information on your employees
- Encourage employees to develop an individual disaster plan for their families
  - Develop payroll/HR policies
    - Will employees be paid if they are unable to return to work?
    - Will employees be given cash advances if needed?
    - Can your employees be paid via direct deposit?
    - If employees have hardships after the disaster, how will you handle leave?
- Obtain and prepare re-entry letters for key personnel and disaster response team to return to the facility
- Develop a plan for employees to work from home if your facility is closed for an extended period of time; include clear expectations

Step 2: Vital Records

A document retention and storage program is critical to any disaster recovery program. The organization must determine what to keep and what to be stored off site. Much of what to keep will depend on legal requirements for your organization and the disaster recovery team should consult with tax advisors and legal counsel to determine what records you are required to keep.

Questions to ask in this phase of the organization planning include:

- Does the organization have a fireproof, crush-proof safe or file cabinet to store crucial documents?
- Have all critical documents been scanned and stored on a CD, on the intranet, the cloud, or in a password protection section of your website?
- What is your organizations intellectual capital? In other words, who knows about your services, your administrative functions?
- Who could provide this information if those with the answers were unavailable? Does anyone else know these answers/ information? Is it written?
- Is all insurance coverage current and does the organization have a clear understanding of the policy coverage, exclusions, deductibles, etc.?

Step 3: Information Technology

With the increased dependence on computers and technology, a computer crash can be just as devastating as a natural disaster. If computers are integral to your organizations operations, below are steps to take to as part of your disaster recovery plan.

- Inventory all computer hardware and software
- Create a diagram of your network structure (your IT consultant can assist in this function)
- Maintain a list of vendors and contact information for all IT functions including website hosting, e-mail service, cell phone service, etc.
- Document all passwords needed to access files and data – store this information off-site.
- Know how to program phones to forward numbers, change voice mail messages, retrieve voice mail messages and any other functions
- Have the ability, and know how, to update your website from outside your office
- Train employees on how to access their e-mail from alternate sites. In addition to your organization e-mail, set up a free e-mail account for emergency use. Document and share this e-mail with key personnel.
- Have a plan for data back-up and make it part of your office routine.

It is recommended that organizations utilize the services of an IT consultant to assist in evaluating the organizations needs and developing this portion of the disaster recovery plan.

Step 4: Physical Premises

Whether you lease or own your premises, it is important to create a site map and check list for your physical premises. Steps to include:

- Evaluate and document your space including floor plans, fire extinguisher locations, emergency exits, designated escape routes and areas of refuge. Are the batteries for emergency lighting checked regularly? Do electric door/ keypad locks have manual bypass locks? Do people know how to use fire extinguishers? Are your emergency routes posted? Is there a "safe room" to move computers and records on site during an emergency?
- Review insurance policies for coverage, deductibles, limits, etc.
- Keep an updated inventory of all furniture and equipment
- Photograph all property kept on site and off site. This is valuable to have for insurance claims, particularly in cases of total destruction.
- Develop a relationship with contractors and other service providers who can be available to assist with restoration as soon as it is safe to return to your facility. Include the contractors' contact information in your plan.

Step 5: Communications

During and after a disaster, an organization needs a system in place to communicate, whether to let employees know the organization is closed or to contact certain personnel. This can be as simple as a phone card that employees carry listing names and phone numbers, or it can be radios or cell phones with emergency contacts stored.

- Create a contact list for all employees including every known way of getting in touch. Include home and cell phone numbers, alternate e-mail addresses, and phone numbers of relatives and friends who might be an evacuation location for employees.
- Organizations should make alternate contact arrangements should phone be unavailable. Arrange for a way for staff to get information on what to do, where to report, etc. This can be done with a call-in number outside the impacted area, or through a website that can be updated by the disaster preparedness team.
- Beyond employees, have a plan to get messages out to the media if necessary. Identify a spokesperson that will interface with the media and develop relationships prior to a disaster.
- Prepare a script as part of your plan including how to communicate with your organization, arrangements that have been made to continue your services, etc.
- Have contact information for all clients, volunteers, and any others that depend on your organization.
- Consider setting up a corporate Facebook page. With the increased use of social media, Facebook is an excellent way to stay in touch with employees, clients, and vendors.

See pages 6 & 7 for helpful checklists

Maureen Clary, CPM
Director, Asset Management Services

Maureen serves as Corporate Realty's Director of Asset Management Services as well as General Manager for the Benson Tower real estate portfolio in New Orleans.

Maureen has over twenty-five years of experience in commercial real estate and development including office, retail, industrial and multifamily properties. Prior to joining Corporate Realty, Maureen served as Executive Vice President of Latter and Blum Property Management overseeing a portfolio of 5 million square feet of office and retail properties and 5,000 multi-family units and as Vice President and Director of Real Estate Services for the University of New Orleans Foundations. In that capacity, Maureen worked with the University partners in the development and asset management of Foundation real estate, as well as the ongoing development, construction and operations of the 35-acre UNO Research and Technology Park and other Foundation public/private partnerships.

Additional Resources:

State Hazard Mitigation Plan
getagameplan.org/planMitigate.htm

Federal Emergency Preparedness
ready.gov/planning

Ready Rating (from American Red Cross)
readyrating.org

Business Continuity Planning
disastersafety.org/open-for-business

DISASTER PREPAREDNESS CHECKLIST

Getting Started **Date Completed**

- Assemble a Disaster Planning Team ____________
- Develop a Disaster Response Team ____________
- Update Policy and Procedure Manual ____________
- Train Employees on the Disaster Plan ____________

Human Resources

- Update information on all employees ____________
- Create communications list for employees ____________
- Develop payroll policies ____________
- Develop policies for return to work ____________
- Encourage employees to create family plan ____________
- Create a plan for telecommuting ____________
- Have a plan to handle payroll off-site ____________

Vital Records/Information Technology

- Store set of vital records on site in fireproof/waterproof ____________
- Store set off site – on intranet, CD, flash drive ____________
- Inventory computer hardware and software ____________
- Have laptops available for key employees ____________
- Create diagram of network structure ____________
- Create list of IT vendors-website, email ____________
- Document passwords-save offsite ____________
- Learn remote access for voice-mail service ____________
- Have ability to update website remotely ____________
- Have a plan for regular back-up of date ____________
- Set up free email service for emergency use ____________
- Train employees on how to gain access to website/e-mail ____________

Physical Premises

- Evaluate your facility and create a facility site map ____________
- Inventory all furniture and equipment (on-site and off-site) ____________
- Photograph all furniture and equipment ____________
- Identify potential “safe rooms” within your facility ____________
- Acquire and store an emergency tool kit and materials ____________
- Acquire and maintain a first aid kit ____________
- Develop evacuation plan for emergencies ____________
- Develop plan to secure building in event of evacuation ____________
- Develop plan to continue service at alternate site ____________

Communications

- Create contact list for all employees ____________
- Create local media contact list ____________
- Create client, volunteer contact list ____________
- Designate spokesperson ____________
- Designate coordinator to update website, VM, etc. ____________
- Prepare script ____________

DISASTER RECOVERY CHECKLIST

Human Resources **Date Completed**

- Convene Response Team and Evaluate Situation ____________________
- Clarify roles and responsibilities/chain of command ____________________
- Determine emergency needs of employees ____________________
- Communicate expectations to employees ____________________
- Provide constant updates if possible ____________________
- Obtain emergency cash ____________________

Vital Records/Information Technology

- Assess status of all communication equipment ____________________
- Assess computer and other IT capacity ____________________
- Access stored or off site data and begin restoration ____________________

Physical Premises

- Have re-entry authorization to gain access ____________________
- Evaluate and secure premises as soon as safely possible ____________________
- Activate emergency contractor as needed ____________________
- Post information on door of premises with key contact information ____________________
- Take pictures and video of damage ____________________
- Contact insurance company to report damage ____________________
- Follow insurance company guidelines for clean-up ____________________
- Activate plan for alternate site if damage is too great ____________________
- Keep a detailed report of all activity ____________________

Communications

- Initiate media plan if needed ____________________
- Update website and voice mail messages often ____________________
- Communicate with clients and stakeholders regarding status ____________________
- Keep staff informed of all communications ____________________