YOUR COMPANY

Your logo

Business Continuity and Disaster Recovery Plan

Revision: January 29, 2014

YOUR COMPANY
Business Continuity and Disaster Recovery Plan

Table of Contents

YOUR COMPANY
Business Continuity and Disaster Recovery Plan

Introduction

The Senior Management of YOUR COMPANY (hereinafter referred to as the Organization) recognize the need to protect employees during an emergency and to have detailed recovery plans to provide for the continuity of operations of the Organization in an emergency or disaster situation. This document has been developed to meet those needs and it will be used in the event of a disaster or emergency.

This Plan could be implemented as a result of many types of disasters, including natural disasters such as flood, fire or severe weather, technical disasters, such as equipment or power failures or human events, such as terrorism or vandalism. Since the number and type of emergencies that could occur is quite numerous, the Plan is written to cover a major emergency or disaster and the Plan will be adapted to the situation or disaster faced.

Purpose and Scope

It is the intention of senior management to continue service to its customers in spite of any unplanned and extended interruption of primary business functions. The purpose of this document is to designate who will be responsible for making critical decisions during an emergency situation and to provide guidelines to be followed in an emergency. Plan assumptions are defined below.

- The Plan seeks to minimize the financial exposure and vulnerability of the Organization.
- The level of recovery for any specific function is determined by the critical nature of the various business functions as well as the need to maintain public confidence and credibility.
- The Plan will be amended as changes in the business environment occur.
- The Plan will be reviewed my management, internal and external auditors and regulatory examiners as requested.

Plan Objectives

The major objectives of this Plan are listed below.

1. Protection of personnel
2. Protection of property and records
3. Continuity of management
4. Restoration of critical function within 24 – 48 hours
5. Restoration of essential functions within 72 hours

6. Eventual resumption of normal operations including all non-essential functions

Management Succession

In an emergency situation following a major calamity, procedures may be needed to ensure that the Organization's remaining officers have the authority to direct immediate recovery operations to speed the resumption of vital operations. The following specific measures are to be implemented to maintain continuity of leadership.

Executive Succession

In the event of an emergency, the officers and employees of the Organization will continue to conduct the affairs of the Organization under such guidance from the senior management as may be available subject to conformance with any governmental directives during the emergency.

Senior management shall have the power, in the absence or disability of any officer, or upon refusal of any officer to act, to delegate and prescribe such officer's powers and duties to any other officer or director.

If the Chief Executive Officer cannot be located or is unable to assume or continue normal executive duties, then the authority and duties of the CEO shall, without further action of senior management, be automatically assumed by one of the following persons in the order designated.

- Managing Director
- Consulting Services Director
- Director of Operations and Technology Services
- Chief Financial Officer

In any emergency, all officers and employees should proceed to the Organization or to the relocation site as appropriate. As soon as possible, the person whose name appears highest on the succession list will become the Organization's acting Chief Executive Officer until the arrival of someone higher on the succession list. At all times, the available person whose name is highest on the succession list will be the Organization's acting Chief Executive Officer.

Administrative and Other Personnel Succession

The administrative and personnel succession shall follow a similar plan where succession for each department will flow from the Department Manager to the next highest level employee in the department in the event the Department Manager is unable to assume or continue normal duties.

Emergency Team Assignments and Responsibilities
Emergency Response Management Team (ERMT)

Senior Management of the Organization has delegated the responsibility and authority for the institution, operation, monitoring and revision of the Plan to the Emergency Response Management Team (ERMT or the "Team"), also known as the Disaster Team. The Team members are listed in **Appendix A**. Senior Management is committed to providing the Team sufficient support and resources to carry out the responsibilities and duties set forth in this Plan.

The Team is also responsible to assess the nature of damage sustained in the event of a disaster situation and to implement the Plan. Each member of the Team will maintain a copy of the Plan to ensure easy and quick access in the event of a disaster situation. In addition, each member will be responsible for informing the other members of the Team regarding any plans for extended absences (three days or more) from the immediate area. If an extended absence is anticipated, members must be informed of the absent member's itinerary.

The basic responsibilities of the Team are as follows.

1. Develop, oversee and monitor the Organization's Plan.
2. Define the critical and essential functions of the Organization and determine in what order the functions will be restored.
3. Analyze the Organization's exposure to the various types of threats and vulnerabilities and establish emergency procedures to follow.
4. Establish a chain of command for notifying people in the event of a disaster.
5. Develop communication procedures to adequately inform and direct all levels of management and other personnel during emergency situations.
6. Develop procedures to take care of customers during an emergency.
7. Evaluate the adequacy of critical technology service providers' contingency plans.
8. Ensure that backup sites are supplied with appropriate materials.
9. Authorize special assignments as needed.
10. Approve expenditures relating to the Plan.
11. Evaluate the Organization's insurance coverage to ensure that it is up-to-date and adequate for current needs.
12. Adequately train personnel in disaster preparedness and evacuation procedures.

13. Ensure that the Plan is tested at least annually.
14. Meet at least annually to review and update the Plan.
15. Periodically report findings/recommendations to the Board for its review.

ERMT Areas of Responsibility

The first person to recognize the disaster will contact the appropriate Emergency Agency Contact List (a listing is provided in **Appendix B**) and the Team Leader and other Team members. Once notified, Team members will gather at the location of the disaster or alternate location if necessary and will begin to carry out responsibilities defined below.

Emergency Coordinator – NAME OF COORDINATOR

- Manage and direct the recovery effort, coordinate teams, monitor recovery schedule, and serve as contact person for recovery services.
- Coordinate financial resources necessary to respond to the disaster and authorize expenditures.
- Works with Public Relations for all media communication.

In addition to the broad responsibilities of the designated Team leaders, individual Team members will carry out responsibilities defined below according to their area of assignment as shown in **Appendix A**. Each Team member may appoint individuals to serve as members of a specific recovery team as needed. If a recovery area leader appoints a team, he or she is responsible for notifying the ERMT of the employees that make up the appointed team.

Damage Assessment

- Evaluate the initial status of the damaged area and estimates both the time to reoccupy the facility and the salvage value of the remaining equipment.
- Oversee the salvage of equipment and data; identifying which resources remains.
- Determine the future utilization of salvaged items in rebuilding and recovery from the disaster.
- Coordinate clean up at the disaster site.

Safety

- Ensure that first aid is available at the emergency site.
- Ensure that all employees are accounted for.
- Notify employees' families of emergency situation.
- Handle all personnel and injury issues.

Security

- Protect the assets and records of the Organization by
  - Locking all doors as needed
  - Gathering all purses and valuable items that may have been left behind
  - Distributing valuables to owners or placing in a secure location
- Contact security guard if needed.

Communications

- Initiate calling tree for contacting employees (see **Appendix C** – Employee Contact List).
- Notify the insurance company (see **Appendix D** – Summary of Insurance).
- Notify regulatory authorities.

Facilities and Supplies

- Coordinate with vendors on the replacement of equipment and supplies (see **Appendix E** – Offsite Storage and Disaster Supplies).
- Locate a temporary working facility, if necessary.

Information Technology Recovery

- Implement all detailed recovery procedures for information technology functions.

Information Technology Recovery Team

Members of the ERMT have been assigned responsibilities for specific areas. In addition to the ERMT, an Information Technology Recovery Team has also been established to deal specifically with recovery of technology systems and operations of the Organization. Members of this team are also listed in **Appendix A**. This Team shall be directly responsible for the actual restoration of business functions by implementing defined recovery procedures of the Plan.

Functional Area Response Members (FARM)

Employees from every area of the Organization have also been designated as Functional Area Response Members (FARM) in **Appendix A**. These individuals have the basic responsibilities defined below.

1. Establish detailed recovery procedures to be followed in an emergency or disaster situation.

2. Assure that their remote locations are implementing departmental or remote location backup procedures and storing backup media properly.
3. Restore communications within their respective remote location.
4. Assure that there is ongoing training for new personnel.
5. Account for each employee in their area in the event of an emergency.

FARM members will coordinate with ERMT to assure that procedures have been established for the remote location to be able to function after an emergency or disaster.

Under the overall direction of the Emergency Response Management Team, support is provided to assist an area's recovery by Functional Area Response Members. These teams work in conjunction with the Emergency Response Management Team. They work to restore services and provide assistance at the operation level to the area affected by the problem condition and to restore services.

Risk Assessment and Business Impact Analysis

In addressing contingency planning, Senior Management is aware of the potential risks that may arise. Disruption to operations can impact the Organization for both the short term and long term. There are various types of risks and many scenarios that could put the Organization at risk. A detailed analysis follows defining the risk areas and an analysis of possible scenarios with probabilities and impact levels assigned.

Types of Risk

Appropriate planning is done to minimize the following risks. Any combination of these risks is present when an emergency occurs, disrupting normal operations of the Organization.

Compliance risk
In an emergency, it is important for the Organization to maintain legal compliance with various appropriate regulations as well as compliance with the organization's data processing emergency and disaster recovery preparedness policies. The Plan will take into account compliance and regulatory issues in the development of all recovery procedures.

Transaction or operational risk
Transaction or operational risk can impact earnings or capital due to problems with service or product delivery resulting from an emergency situation. Transaction or operational risk occurs in the delivery of all products and services, and it may be addressed through consideration of all aspects, including data input, data processing, data output, Internet based services, and network services. People, equipment, systems, data files, and other significant elements of the Organization's processing

ensure the restoration of processing and service within a short timeframe and are critical to customers of the organization and the viability of the Organization.

Strategic risk
Strategic risk management involves addressing the potential adverse business impact to the organization, both internally and externally, that may occur if the Organization is unable to restore network, data processing operations, and related functions within an acceptable time frame. If the strategic risks related to data processing disaster recovery are not understood, addressed, and managed in terms of preparedness, the Organization may not be able to address the risks and related solutions in the short term, resulting in economic and market losses.

Reputation risk
Developing and retaining marketplace confidence in handling customers' transactions in an appropriate manner, within an acceptable time frame, as well as meeting the emerging needs of the customer base and community, for example, after a disaster, are important in protecting the safety and soundness of the Organization.

Scenarios and Probability

The Organization faces a number of emergency situations that could interrupt business. The Organization could experience an interruption as a result of natural causes, unnatural causes or technological causes as summarized below.

Scenario	Probability	Potential Impact
Natural Causes		
Fire	Medium	High
Flood	Low	High
Hurricane	Very Low	High
Tornado	Medium	High
Earthquake	Very Low	Medium
Other severe weather	High	Low
Air contaminants or hazardous spills	Low	Low
Human Threats & Malicious Activity		
Civil strife	Very Low	Low
Virus	Medium	Medium to High
Network security attack	Medium	Medium
Fraud, theft or blackmail	Low	Medium
Arson	Low	High
Vandalism	Low	Medium

Terrorism	Very Low	High
Bombing	Very Low	High
Technical Threats		
Hardware or software failure	High	High
Communications failure	Medium	High
Power failure	High	Medium

Procedures are required for any scenario that is rated to have either a high probability or high impact and procedures may be developed for other scenarios as well. Emergency procedures for the high-rated natural causes, human threats and malicious activity are included in the Emergency Procedures section of the Plan. Procedures for recovery of complete business functions are included in the Functional Area Recovery Procedures section of the Plan. Procedures for recovery from all technical threats are detailed in the Information Technology Recovery Procedures of the Plan. Procedures for recovery of remote location locations are included in the Remote Location Recovery Procedures section of the Plan.

Some scenarios that are not rated to have a high impact or high probability may actually result in the need to follow either emergency procedures, such as a building evacuation, or recovery procedures, such as restoring an electronic system. Defined procedures for high probability/impact scenarios will be followed as appropriate should another scenario not specifically addressed occur.

Assessment of Functions

Every Organization function and department has been considered and evaluated as to the downtime allowable and recovery time objectives. Functions have been categorized according to the disruption that would be caused if the function were not available and have been classified using the following categories.

Critical - the loss of the function would seriously jeopardize operations after one day disruption of service

Essential - the loss of the function would seriously jeopardize operations after a one week disruption of service

Non-Essential- the performance of the function is convenient and necessary to customers and the Organization but the lack of such function does not seriously detract from operating capabilities

Critical Functions

The following areas have been identified as those critical to the overall operation of the institution and contingency or recovery plans must be maintained for these areas.

- Core business processing – Communications via Cell, Land Line or E-mail
- Data Center (or server room) – What systems are in your DC (including WAN connectivity)
- Human Resources – Payroll
- Internet Services including External Website

Essential Functions

The following areas have been identified as those essential to the operation of the institution and recovery plans may be maintained for these areas.

- Remote Location Communications (Phones & External Telecommunications)
- Primary Email (Use alternative if available)
- Operations, Administration and Accounting - Accounts Payable
- Network – User data folders and other applications (SharePoint)
- Printing
- Facilities

Non Essential Functions

- Company Operations, Other accounting functions not listed above, Regulatory Reporting
- Investments and Asset Liability Management
- Human Resources - All functions other than payroll
- Demo and Test Virtual Machines
- Customer Access to Virtual Services – White Papers and Tutorials

Recovery Priorities

Efforts will be devoted restoring Critical functions first. Once Critical functions have been restored, efforts will be devoted to re-establishing Essential functions. After all Critical and Essential functions have been restored, attention will be given to restoring Non-Essential functions and services.

Critical functions will be restored for the most part in the order the functions have been listed however recovery efforts will more than likely be simultaneous for all Critical functions.

Classification of Disasters

The impact of a disaster will be assessed by the ERMT and classified as follows.

- Level 1 - No interruption in operations.
- Level 2 - Some facility and computer equipment damages observed, but operations can be resumed within 8 hours.
- Level 3 - Moderate damage to the facility and/or the computer equipment is observed, but operations can be resumed within 8 to 48 hours.
- Level 4 - Major facility and computer equipment damage is observed with interruption in operations for over 48 hours. All personnel and functions must be moved to the Designated Alternate Site.

Recovery procedures have been developed considering the seriousness of a disaster and the levels described above. Most functions have recovery procedures that will be used in all Level 1, 2 or 3 disasters and then additional procedures to be used for a Level 4 disaster. For example, manual processing will be used for most emergencies lasting up to 48 hours (Levels 1, 2 and 3) before processing is actually moved to the offsite location due to a Level 4 disaster.

Declaring a Disaster

Once an emergency or disaster has occurred, the Alternate Emergency Coordinator, the ERMT member assigned with Damage Assessment responsibility, will assess the damage in order to determine the level of the disaster. A disaster will be declared only if the damage is determined to be major, sufficiently warranting a Level 4 status. The ERMT Team Leader, Emergency Coordinator and Alternate Emergency Coordinator will meet after the initial damage assessment to collaborate on such a decision. At that point a disaster will be declared, emergency and recovery procedures will be implemented, and Organization functions will move to the alternate location defined below. Two of these individuals (Team Leader, Emergency Coordinator or Alternate Emergency Coordinator) may also declare a disaster if all three are not available to discuss the situation.

Alternate Locations

If main office is temporarily or permanently unable to continue operations, the first location listed below will become the acting head office of the Organization. If the first location is not available, the second location listed will become the acting head office of the Organization.

- Primary Office: (Location)
- Secondary Office: (Location)
-

Records Protection

The Organization has implemented a number of systems and procedures to protect the records of the Organization. Both electronic and paper records must be protected. The Organization should be able to reconstruct its position and account relationship with customers following an emergency. To achieve this, the Organization archives various records in locations not in the immediate area of the Organization. A copy of all data files and software is retained along with photocopies, microfilm or optical disks containing other Organization records, such as notes and collateral.

*<Insert details of how and where records are stored. Data files that are stored offsite are already defined in **Appendix E**, so a reference to that Appendix may be sufficient for defining storage of application software and data.> HOW ARE THESE STORED? OR ARE THEY STORED ANYWHERE ELSE?*

Insurance

The Senior Management must review the insurance coverage for the Organization on an annual basis. The Organization believes that it has sufficient insurance coverage to guard against loss from risks that cannot be completely prevented. In reaching this conclusion, the Organization assessed the possible hazards and the potential dollars at risk versus the costs of insuring.

In the event of a disaster that requires insurance claims to be submitted, such claims are to be filed immediately. All proceeds from the payment of the insurance claims will be utilized to replace or restore damaged structures and equipment at the first possible occasion. A list of the Organization's insurance carriers and the coverage provided can be found in **Appendix D**. A list of our Inventory of Systems is included in **Appendix F** and a Summary of Telecommunications Circuits is found in **Appendix G**.

Employee Training

Testing of the Plan is an essential element of preparedness. All Organization employees will be trained in emergency procedures annually. In addition, employees that have roles defined in the Plan will be trained to carry out their individual responsibilities defined in the Plan.

Plan Testing

The Plan will be tested annually. A summary of the testing results will be presented to Senior Management. A copy of the most recent Disaster Recovery Testing can be found in **Appendix H**. Testing will include, at a minimum, the following areas.

- IT Recovery procedures for all critical applications
- Emergency procedure testing
- Remote location emergency and recovery testing

Plan Maintenance

The Plan will be reviewed annually to determine if revisions are needed. New services, changes in location, and changes in vendors will be considered during the review. Changes will be made and the revised Plan along with a summary of all Plan testing will be presented to Senior Management. Each time revisions are made, updated copies will be distributed to all Team members and an updated copy will be taken offsite.

Emergency Procedures

General Overview

Upon information being received of any of the following natural disasters, the ERMT working with the Emergency Coordinator will review the situation and declare the recommended plan for the situation. If the timeline of the disaster is sufficient to allow staff to return safely to their homes, employees may be asked to continue working until close of business, which allows for time to make last minute preparation before shutdown of the institution. However, if an immediate situation arises, the Emergency Coordinator will declare specific actions.

Emergency Evacuation Procedures

There may be instances because of fire, bomb threats, etc. when it will be necessary to evacuate the building as rapidly as possible. When an employee becomes aware of an emergency, he/she must immediately notify his/her supervisor or a senior member of staff at the branch location if his/her supervisor is not at that location. That person in turn will notify Senior Management and Civil Authorities.

Managers are responsible for supervising the evacuation of their respective areas. Personnel are reminded that personal safety is of first and foremost importance in these emergency evacuation procedures. Steps that cannot be safely completed should be ignored.

1. Escort all customers out of the office immediately. Office exits will then be secured and no one shall be permitted to enter the office. Secure doors when notified by the Senior Officer to do so.

2. All employees should secure their work area and then proceed through the front door. If the front door is not accessible, then, you should proceed through an alternate exit if available.

3. Supervisors should attempt to secure all valuable records in a cabinet or locked desk.

4. Employees should shut down or lock workstations before exiting the building if time permits.

5. The IT Department should follow the Emergency Shut Down Procedures described in the next section.

6. All staff should proceed with customers to disaster-designated meeting places outside the building. Each branch office has a different meeting location outside the building, please see your local office emergency procedures.

7. DO NOT USE ELEVATORS. Evacuate the premises using the stairwells.

8. Do a quick visual inventory before leaving to see if any staff or customers are still on site. DO NOT TRY TO RESCUE THEM, proceed outside and immediately advise a member of Management of anyone left inside. It is important to be specific if someone is missing, providing the location and last time that person was sighted. If the person's name is known or some description is possible, please try to remember as you leave the premises. Department Heads must verify that all personnel are accounted for.

9. Do not reenter the building until instructed to do so.

If the building is not vacated, staff should remain calm and stay within their work areas until further instruction is provided. The ERMT should immediately proceed to a conference room to discuss the disaster, implement the plan, and initiate individually assigned responsibilities.

If after hours, the individual contacted will initiate the calling tree to ensure that all members have been notified. Depending on the type of disaster, the ERMT will either proceed to the Organization to assess damage or initially meet at a designated nearby location.

Add emergency procedure for tornado.

Emergency Shut Down Procedures

The following procedures are to be followed in an emergency. A copy of these procedures is posted on the door the computer room and all IT personnel have been instructed to follow these procedures.

For each location in your building(s), specify how you would shut down your IT Equipment in the case of an emergency

Recovery and Restart Procedures

The following procedures are to be followed after an emergency to restore systems. A copy of these procedures is posted on the door to the computer room and all IT personnel have been instructed to follow these procedures.

Same thing here, outline how you would turn your items back on again.

Medical Emergencies

During a medical emergency, employees should use the following guidelines.

1. **Remain Calm** and immediately call for rescue squad or ambulance.

2. To insure adequate breathing, open and maintain the victim's airway by gently tilting head back. If victim is NOT breathing, immediately begin mouth-to-mouth resuscitation.

3. Check and periodically recheck the victim's carotid pulse in the neck, using two fingers. If pulse is not present, immediately begin CPR.

4. Stop all obvious bleeding by applying direct pressure over the wound with your hand. If available, use a clean cloth or bandage.

5. Do not move victim unless a hazard is present. Keep the victim in a quiet, comfortable position.

6. Loosen all tight clothing.

7. Keep victim warm - do not induce sweating.

8. Give no fluids - except very small sips of water, only if requested by the victim.

9. Elevate victim's legs slightly, unless an injury is present on the chest or head.

10. Comfort and reassure the victim constantly.

11. For all on-the-job injuries, notify your supervisor as soon as possible.

Loss of Electrical Power

A loss of electrical power can prove to be a serious situation for all institutions. Not only does it pose a security threat and loss of communication, but also physical threat with the loss of air or heat.

As soon as a power failure has occurred, a member of the ERMT will contact or designate an employee to contact the power company to report the outage and determine if there is an expected time for restoration of power. Based upon the information obtained, a decision will be made as to the next steps to be taken.

In cases of extended loss of power, the ERMT may declare an emergency and the premises vacated. If the building is to be vacated, employees should follow the basic emergency evacuation procedures described above. A sign stating that the Organization has been closed will be posted. The local police will be contacted to alert them of the power failure and the evacuation of the building. The remaining remote locations also will be notified regarding the status of the outage for customer inquiries.

Systems that are on UPS battery backup should be monitored. If the outage is over 30 minutes, plans should be made to shut down servers according to the procedures described above.

Fire

In the event of a fire that IS NOT AN IMMEDIATE DANGER, the following steps should be taken:

1. Notify Management immediately.

2. Set off the nearest fire alarm to alert others.

3. If the fire has not advanced too far, attempt to control it with a fire extinguisher.

4. If the fire is in the computer room and the IT manager is not present at the time of the emergency, immediately notify him if possible.

5. If the fire is located in the computer room and equipment is not in immediate danger and accessible. Shut down equipment according to the procedure listed above.

6. Exit the building, closing doors and windows behind you when leaving your work area.

7. When exiting the facility, check all closed doors for extreme heat before opening any doors. Lightly touch the door to feel for extreme heat. If the door is not extremely hot, cautiously open the door, and when deemed safe, enter the corridor and close the door behind you. If the door is extremely hot, DO NOT OPEN THE DOOR, but retreat as far away from the door and adjoining wall as possible and signal for help from a window.

8. Notify the fire department.

If the fire is determined to be an immediate threat to personal safety, personnel are instructed to implement the evacuation procedures in this policy, closing all doors to the fire area, and notifying the fire department when they are safely away from the area.

Flood or Water Leakage

The following procedures should be followed in the event of a flood or water leakage.

1. Notify Management immediately.

2. Shut down all electrical equipment, by turning off the appropriate circuit breakers after a normal shutdown. The degree of ‘normal’ shutdown will depend upon judgment and under no circumstances should an employee be subjected to any

greater danger than necessary.

3. Cover equipment with protective plastic sheets, if available.

4. Move all data stored on removable media to a safe place.

5. Move critical workstations and servers to a safe place if time permits. At a minimum, any workstations located on the floor should be moved from the floor to the desk.

6. Depending upon the severity and location of the flood, a member of the EMRT, the Department Head or Remote Location Manager will contact the appropriate persons to stop water entry if possible and/or to remove water.

7. Judgment is to be used to determine the severity of the situation, which will dictate further actions to be taken.

Natural Phenomena

In case of a natural disaster such as a hurricane or flood, the Organization will allow employees to return home within a reasonable time to secure themselves and their families. Employees are to make every effort as soon as possible to notify Management of the Organization if he/she is a victim of such a disaster.

Tornado Procedures

Employees of the Organization are to move to the center of the floor on which they work away from windows and glass if they are alerted of an impending tornado. Shelter should be taken in rooms without windows if possible at the most interior portion of the building.

List here each office and where to go.

Terrorism or Bomb Threat

If an employee suspects that a bombing device is present, extreme caution must be exercised and the following steps should be considered.

1. Notify Management to immediately call 911.

2. The Department Supervisor should contact the most senior member of the ERMT.

3. Determine the answer the following questions:
    a. Is this an isolated circumstance?
    b. Is the threat specific?
    c. Is time imminent?
    d. Is the threat plausible?
    e. Is the caller convincing?
    f. Is the danger avoidable?

4. The ERMT is responsible for inspecting the premises to locate unidentifiable or unexplained objects or packages only under the direction of emergency workers. Consider such items as briefcases, luggage, shopping bags, purses, and wrapped packages. Be as thorough as possible, time permitting. In general, any place with public access such as restrooms, conference rooms, and unlocked storage rooms, public lobbies, trashcans, elevators, or stairwells, etc. should be inspected.

5. Use extreme CAUTION and do not touch or attempt to move a suspicious object.

6. Take appropriate action to protect employee and customer property.

7. Explain the situation to other employees in an effort to avoid panic and prepare for orderly response.

8. Evaluate the possibility of evacuating.

Summary of Basic Disaster Plans

<Insert a very short summary of the Organization's basic plans in this section. A few sample paragraphs are provided as an example.>

The Organization has an agreement with XYZ Disaster Center for backup processing. In the event of a disaster, the Organization's basic plan is to operate in a mostly manual environment for up to two days. If recovery cannot be expected within two days, processing will likely be moved to the offsite recovery center.

OR

The Organization's core processing is outsourced to ABC Vendor. The Organization relies upon ABC Vendor's disaster planning to provide processing

the event the vendor experiences an emergency. If the vendor is down for up to two days, all processing will be done manually. If the Organization is damaged or not operational, the Organization can send employees to ABC Vendor's location since it is in close proximity. Employees will be allowed to access systems there on a temporary basis. A new file server will be ordered to restore the network if necessary.

Functional Area Recovery Procedures

On the following pages, documentation of functional areas and associated recovery procedures are included for the areas listed below.

- Administration
- Accounting
- Consultants
- Client Relations
- Sales & Marketing
- Cloud Services
- Human Resources

<Insert detailed recovery procedures for all functional areas listed above using the Blank Functional Area Recovery Procedures document shown on the following page.>

YOUR COMPANY
Business Continuity and Disaster Recovery Plan

Functional Area Recovery Procedures

Functional Area	**Administration**
Classification of Functions	Critical Functions Essential Functions Non Essential Functions
Emergency Procedures Specific to Functional Area	
Systems & Software Relied Upon	
General Resources Needed	

Function	
Supplies and Documents Needed	
Recovery procedures	

Function	
Supplies and Documents Needed	
Recovery procedures	

Function	
Supplies and Documents Needed	
Recovery procedures	

YOUR COMPANY
Business Continuity and Disaster Recovery Plan

Functional Area Recovery Procedures

Functional Area	**Accounting**
Classification of Functions	Critical Functions Essential Functions Non Essential Functions
Emergency Procedures Specific to Functional Area	
Systems & Software Relied Upon	
General Resources Needed	

Function	
Supplies and Documents Needed	
Recovery procedures	

Function	
Supplies and Documents Needed	
Recovery procedures	

Function	
Supplies and Documents Needed	
Recovery procedures	

Information Technology (IT) Recovery Procedures

Detailed procedures for the actual recovery of business functions, applications and systems are defined in the following pages. These procedures will be followed for all to recover IT systems. The IT Recovery Team will be responsible for implementing the recovery procedures. Some procedures rely upon recovery of other systems and will be referenced accordingly.

<This is a sample list of IT Recovery Procedures that may be generated, so it should be tailored to the Organization's needs. This may include procedures for both critical and essential functions, but at a minimum the critical functions must be included>

- Core Business System
- Network File Server
- Telecommunications
- User Data
- Email

<Insert detailed recovery procedures for all systems listed above using the Blank IT Recovery Procedures document shown on the following page.>

Information Technology (IT) Recovery Procedures

Application or System	
Classification	
Maximum allowable downtime desired by Organization	
Anticipated recovery time	
System details	
Backup and redundancy	
Detailed recovery procedures	

Remote Location Recovery Procedures

On the following pages, documentation of remote location recovery procedures is included.

<List each remote location here – this is a sample only>

- Remote location1
- Remote location2
- Remote location3

<Insert detailed recovery procedures for each location using the Blank Remote Location Recovery Procedures document shown on the following page.>

YOUR COMPANY
Business Continuity and Disaster Recovery Plan

Remote Location Recovery Procedures

Location	**Remote Location1**
Classification of Functions	Critical Functions Essential Functions Non Essential Functions
Remote Location Emergency Procedures	
Alternate Locations	
Systems & Software Relied Upon	
General Resources Needed	
Supplies and Documents Needed	
Vendors Specific to Remote Location	
Recovery Procedures	

Appendix A - Emergency Teams

The Emergency Response Management Team (ERMT) shall be composed of the following individuals.

Name	Title	Position	Recovery Area of Responsibility
	President & CEO	Team Leader	Public Information
	Chief Financial Officer	Emergency Coordinator	Communications
	Personnel Manager	Team Member	Safety
	Remote Location Operations Manager	Team Member	Facilities and Supplies
		Team Member	Information Technology Recovery
	Technology Services Manager	Team Member	Information Technology Recovery

The Information Technology Recovery Team (ITRT) will be composed of the following individuals.

Name	Title	Position	Primary Responsibility
	IT Manager	IT Recovery Coordinator	Network infrastructure
	Operations Manager	Operations Recovery Coordinator	Core System
	Network Administrator	Team Member	Network servers
	Desktop Support Technician	Team Member	Workstations

The following individuals are Functional Area Recovery Members (FARM) of the Disaster Team.

Name	Functional Area of Responsibility
	Operations
	Accounting

Appendix B - Emergency Contact List

Contact	Contact Information
Local Police Department	
Local Fire Department	
Ambulance Service	
Hospital	
Telephone Company	
Gas/Heat Company	
Electric Company	
Building Manager	
Building Security	
FEMA Regional Office	
Media	
Newspaper	
Television Stations	
Radio Stations	
Insurance Agent	
Regulatory Agencies	
Hotsite Vendor	
Generator Vendor	

Appendix C - Employee Contact List

Contact information for all Organization employees is documented below. Each Department and/or Remote Location Manager will be responsible for notifying all employees within their Department or Remote Location of the emergency situation.

Create or insert Phone Tree here

Employee Name	Home Phone Number	Cell Number	Emergency Contact Name & Number	Alternate email address

Appendix D – Summary of Insurance

Below is a summary of the Organization's insurance coverage.

Insurance Company / Agent				
Address				
Phone				
Fax				
Email				
Type of Insurance	**Policy No.**	**Deductible**	**Policy Limits**	**Coverage (General Description)**

Appendix E - Offsite Storage and Disaster Supplies

General Supplies Inventory

These general supplies are maintained at the Main Office and at each remote location in the <*insert primary supply area*>.

- NOAA Weather Radio
- First Aid Kit
- Flashlights/Batteries
- Waterproof Plastic Bags
- Camera/Film
- Pens/Pencils/Paper
- Small supply of water & nonperishable food
- Tool kit (basic tools, gloves, etc.)

Key Operations Vendors

In addition to the general supplies listed above, the following items are also maintained in <*insert location here*>. Detail supplies for each Remote Location and Department are listed within the Remote Location and Functional Area Recovery Procedures.

<This is a sample list. This list is compiled after each functional area and remote location determines the supplies needed. The supplies for each functional area or remote location do not need to be listed individually here. The forms or supplies can be placed in a large envelope and labeled then referenced here.>

Item	Supplier/Person Responsible
Letterhead and envelopes	XYZ Printing Company 123 Main Street MyCity, LA (225) 333-1234
Accounting Supplies	
Data Processing Supplies	
Operations Supplies	
Add Disaster Companies	

Backup Drives and Software Inventory

The following backup drives and recovery items are retained at *<list offsite tape storage>*. These items are stored in *<a locked fireproof cabinet>* at the offsite location. *<List individuals>* are the only individuals that can access the items as the offsite location.

Backup Drives

- Daily backup tapes for core business system (two week rotation of 2 tapes for each day)
- System save backup tapes (one for each of previous 12 months)
- Network backup tapes (two week rotation, 1 DLT tape for each day)
- Month end network backup tapes (one for each of previous 12 months)
- Etc.

Software

- All software is able to be re-downloaded from the Internet all local copies are recoverable.

Other Recovery Items

These items that are needed for recovery are also retained offsite.

Item	Responsible Party
Copy of Business Continuity and Disaster Recovery Plan	
Organization Policies & Procedures	
Daily Processing Instructions	
Backup Procedures	
Blueprints of the Main Office	

Appendix F – Inventory of Equipment & Computer Systems

A copy of the inventory spreadsheet would be inserted here. Should be updated with all physical servers and switching equipment.

Appendix G – Telecommunications Circuit Information

Below is a listing of the Organization's telecommunications circuits.

Circuit Description	Vendor	Circuit #	Termination Location

Appendix H – Disaster Recovery Testing

<Insert testing information here and update it each year. Use the Blank Functional Area Testing Summary document, Blank IT Recovery Testing Summary document, and Blank Remote location Recovery Testing Summary document.>

Functional Area Testing Summary

Functional Area	
Classification of Functions	Critical Functions Essential Functions Non Essential Functions
Emergency Procedures Specific to Functional Area	
Systems & Software Relied Upon	
General Resources Needed	

Function	
Supplies and Documents Needed	
Recovery procedures	

Function	
Supplies and Documents Needed	
Recovery procedures	

IT Recovery Testing Summary

Application or System	
Classification	
Maximum allowable downtime desired by Organization	
Anticipated recovery time	
System details	
Backup and redundancy	
Detailed recovery procedures	

Remote Location Recovery Testing Summary

Remote Location Tested	
Disaster Scenario(s)	
Summary of Actions	
Persons Involved	
Test Date	
Results	
Plan Changes Needed	
Detailed Testing Procedures	

Appendix I – Disaster Recovery Agreements

<This appendix should include copies of any backup/recovery agreements the Organization has including local proof agreement, core processing disaster backup, mobile facility delivery agreement, etc.>

Appendix J – Technology Service Provider (TSP) Disaster Recovery Plan

<This appendix should include disaster recovery plans for all key vendors (i.e. the systems they provide are considered critical), such as core processing service provider and possibly debit card and Internet Organization providers.>

Credit Card Processors

Bank Information (Accounts)

Appendix K – Technology Service Provider (TSP) Disaster Testing

<This appendix should include disaster recovery testing information for all key vendors (i.e. the systems they provide are considered critical), such as core processing service provider and possibly debit card and Internet Organization providers.>