Nortex Regional Planning Commission

Economic Disaster Recovery Planning

4309 JACKSBORO HIGHWAY
SUITE #200
WICHITA FALLS, TX 76307

Introduction

The region of north Texas is no stranger to disasters. Be it natural or man-made, winter or summer, the challenges are well documented living in an area known for its extremes. North Texas will experience tornados, damaging hail and high winds, flooding, heat and ice storms, all in the same year.

Two major transportation routes traverse North Texas. Highway 287 runs from the southeast corner to the northwest corner of the region and carries over 20,000 vehicles per day. Paralleling the highway is the BNSF railroad. The BNSF is a major supplier of coal and petroleum products for the intermodal traffic of Texas. All of which greatly increases the risk of a disaster that can bring devastation and required long term recovery to North Texas.

Historically, focus would have been on the planning, mitigation and recovery of people and infrastructure. The information contained herein is designed to address business continuity planning and economic recovery. Information has been provided from economic development planners and consolidated to develop this material.

A special thanks and acknowledgment for the State of Maine whose program was used as the foundation for the creation of this project and a special thanks to all who contributed and brought this project to life.

Chapter 1 – Risk Management

Understanding how risk management works is important. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk. Risk is the effect of a natural hazard event. We learned that risk is computed from the probability of the event becoming an issue and the impact it would have on the business. Therefore, (*Risk = Probability x Impact*).

From data collected Economic Development Advisory Committee, which represents the eleven counties involved in our region, 91% of the response cited the lack of water, followed by 67% of the response citing tornados recognized as a high probability of recurring and high impact on communities and businesses. In order to mitigate and reduce the risk of natural hazard events, businesses must realize the importance of implementing a risk management system.

The first step in a risk management process to determine quantitative and qualitative value that will result from a natural hazard event is to perform a risk assessment. The assessments will help determine what information resources exist that require protection as well as understanding the potential risks that may arise from failures, such as loss of information and availability of information. Examples of quantitative value would be the financial decisions, insurance, and loss in terms of dollar amounts and qualitative value would be based on public health and environmental decisions.

The following is a simple step-by-step process to establish risk assessment:

1. Establish the risk assessment team. In small businesses, the team could consist of one or two people.
2. Identify assets to be assessed such as personnel, hardware, software, data, and facilities.
3. Identify the losses that could result from damage to any asset.
4. Identify threats and vulnerabilities such as power failures.
5. Determine cost-effective safeguards that could be implemented to mitigate risk.

For instance, the recent survey Economic Development Advisory Commttee, asked about businesses, if affected by a hazard, "Can your building withstand the impact of a natural disaster, and are your contents and inventory sufficiently protected, so they will not be damaged?" Over 70% of the respondents answered that business would be critical impacted by a disaster. Over 60% responded that loss of staff and customers would be critical in the economic recovery. This clearly indicates the need for businesses to conduct risk assessments. Businesses ranked the interruption of the following services as the most critical to them (in order of priority):

1. Electricity 82%
2. Water 73%
3. Sewer and Wastewater Treatment 73%
4. Transportation 50%
5. Natural Gas & Phone/Internet 45%

All of the above can have an impact as a result of any type of hazard.

Another survey question asked "How long can you afford for your business to be shut down and still survive after a disaster (earthquake, wind storm, etc.) without suffering major financial losses?"

- 50% of the respondents believed that their business could be shut down for up to one week.
- 10% responded that they would immediately suffer major losses.

- 20% responded that their businesses would be fine for up to one month.

Only 25% of respondents to the survey have developed a disaster recovery plan. While 33% report they plan to do prepare a disaster recovery plan, an additional 25% do not believe a disaster recovery plan is necessary. This mitigation and disaster recovery plan serves as a guide to help businesses accomplish this task.

Chapter 2 – Risk Mitigation

The impact of any of the natural hazard events experienced in any of the eleven counties can be minimized through proper planning and preparedness. Adequate emergency plans for communities, businesses, and individuals located in vulnerable areas can also minimize impact. Only 55% of survey respondents have emergency evacuation plans in place while 33% responded they will not make arrangements to relocate the business to another site in case of disaster damage or accessibility issues.

Hazard mitigation planning includes:

- Organizing resources
  - Establishing a planning team
  - Engaging the community in the planning process
  - Securing political support
- Assessing risks
  - Identifying and evaluating the natural hazards,
  - Preparing damage loss estimates
  - Knowing where hazards can affect the built environment
  - Likely outcome of damages and losses
- Developing mitigation strategies
  - Goals and objectives,
  - Focus on identified risks and potential losses,
  - Identify mitigation measures to help achieve goals and objectives
  - Reduce future disaster related losses,
  - Write a plan
- Implementation
  - Adopt plan
  - Implement plan
  - Monitor plan
  - Review plan

Mitigation planning enables business leaders to make good decisions based on sound hazard identification and risk assessment data in order to reduce risks from future hazards.

2.1 Prepare your Business for Disaster. This section will help prepare for a disaster and put your business in a position to survive a disruption. Though each situation is unique, any business can be better prepared if it plans, puts emergency procedures in place, and practices for emergencies of all kinds. It is critical for you to protect your business by identifying potential risks from natural and man-made disasters.

- Most standard insurance policies do not cover flood damage and the resulting loss of income. Check with your insurance agent on how to ensure adequate protection.

- Check with local authorities to find out the 100-year flood level of your structure.

- Consider working with a licensed contractor to raise electrical and HVAC system above the 100-year flood level mark.

- Keep computers, electronics, and important files raised off the floor.

- Consider working with a licensed plumber to install a backflow valve to prevent sewage backup.

- Be prepared to move critical items above flood level during a flood watch.

2.2 Protect your Business from Natural Hazards. Power outages are commonplace during disasters, and they may last for several days. This was the number one interruption most critical to businesses according to the survey. As a result, even businesses that are not severely damaged can suffer losses because of the interruption of normal operations or the loss of perishable stock. You can reduce these losses and speed the recovery process by installing an emergency generator. First, determine which systems and equipment are essential to the continued operation of your business. They may include one or more of the following:

- Heating, Ventilation, and Air Condition (HVAC)
- Industrial equipment and major appliances
- Lights, computers, and other office equipment
- Pumps, including sump pumps, sprinkler system pumps, and well water pumps.
- Alarm systems

Once you have identified the essential systems and equipment, determine how much power they require and check with a generator sales representative regarding the appropriate size and type of generator.

Benefits of using generators:
1) helps to prevent the interruption of normal business operations,
2) helps to prevent the loss of perishable stock, and
3) helps to speed the recovery process.

2.3 Protect Business Records and Inventory. Most businesses keep on-site records and files that are essential to everyday operations. Some businesses also store raw materials and product inventory. The loss of essential records, files, and other materials during a disaster can result in costs and delay to return to normal operations. The longer your business is not operating, the more likely you are to lose customers permanently to your competitors.

To reduce your vulnerability, determine which records, files and materials are most important; consider their vulnerability to damage during different types of disasters (such as floods, hurricanes, and earthquakes) and take steps to protect them, including some of the following basics:

- Raising computers above the flood level and moving them away from large windows,
- Moving heavy and fragile objects to low shelves,
- Storing vital documents (plans, legal papers, etc.) in a secure off-site location;
- Regularly backing up vital electronic files (such as billing and payroll records and customer lists) and storing backup copies in a secure off-site location.

Benefits of utilizing this mitigation strategy will help to prevent the loss of essential business records and files, and protects raw materials and product inventory; helps a quick return to normal business operations; helps to prevent the loss of customers to competitors.

Business preparedness will determine how quickly your company can get back to business after a natural hazard disaster event. As a business owner, you must ask yourself if you are prepared to relocate temporarily; what would happen if my suppliers shut down; and do my employees know what to do in case of an emergency.

A commitment to preparing today will help support employees, customers, the community, the local economy and even the country. It also protects your business investment and gives your company a better chance for survival. The following are steps you can take to get started with emergency planning for your business:

- Learn what kinds of emergencies might affect your company both internally and externally. Find out which natural disasters are most common in the areas where you operate.

- Think about how a disaster would affect your suppliers and customers. A disaster somewhere else can affect your business if you can't get supplies, or can't ship your products.

- Meet with your insurance agent. Do you need flood insurance at your location? Normal business insurance does not cover flooding. Should business interruption insurance be a consideration?

- Develop internal safety plans; evacuation, fire prevention, etc.

- Protect and back up your vital records, both the paper ones and electronic data.

- Make emergency preparedness a priority with you and your employees and your families. If you and your employees know that your families are safe, you can focus on getting the business back on its feet.

- Make a communications plan. How will you communicate with your employees, customers, and suppliers, especially if you are closed down for a while?

- Make a plan for recovery, for getting back in business. Depending on your type of business, this could be an alternate location, emergency power, or other solutions.

- Invest in improvements that will make your buildings and equipment less likely to be damaged.

Chapter 3 – Business Impact Analysis

3.1 Business Impact Analysis

A business impact analysis (BIA) should involve risk assessment, disaster mitigation, and business continuity. The result of a business impact analysis is a report, which describes the potential risks specific to the organization. One of the basic assumptions of a BIA is that every component of the organization is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of funds in the wake of a disaster.

As part of a disaster recovery plan, BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, and so on. A BIA quantifies the importance of business components and suggests appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts on safety, finances, marketing, legal compliance, and quality assurance. Where possible, impact is expressed monetarily for purposes of comparison. For example, a business may spend three times as much on marketing in the wake of a disaster to rebuild customer confidence.

To develop a comprehensive business impact analysis, all business units and departments should be involved. Management should be responsible for coordinating the process and ensuring its effectiveness within the organization. In the event of a natural hazard event, lost revenue can be estimated in the following manner:

- ✓ Lost Revenue: Potential Financial Loss due to missed collections/interest or additional fees
- ✓ Penalties: Loss of business process that would result in fines, penalties, or legal fees due to regulatory requirements.
- ✓ One Time Expense: Loss of business process would result in a one-time expense, such as equipment, a service provider, or materials.
- ✓ Maintaining Service: Is there a cost associated with maintaining service to your internal and external customers without this business function.
- ✓ Recovery of Lost Transactions: Is there a cost associated with recreation of transactions not available on the back-up media? This could be over time or a contracted third party.

- ✓ Backlog Business Functioning: Would overtime or additional staff be required for the business process to address the backlog once the business process is restored?

Business Process:	Day 1	Day 2	Day 3	Day 4	Day 5	Week 2	Week 3
Lost Revenue							
Penalties							
One-Time Expense							
Maintaining Service							
Recovery of Lost Transactions							
Backlog Processing							

3.2 Risk Assessment: Using a ranking and prioritization system for natural hazard events, each risk is ranked in accordance with likelihood and impact. As an example, businesses surveyed ranked power failure as the most critical impact on their business. Other items rated that would have an impact on businesses included damage to buildings, computers, equipment, loss of inventory, etc. The following table could be used to assess risk:

Risk	Consequence	Probability	Impact	Severity
Risk 1	Power Failure	H	H	H
Risk 2	Damage to Computers/Equipment	H	H	H
Risk 3	Loss of Inventory	H	M	M
Risk 4	Loss of Supplier/Vendor	M	M	M
Risk 5	Loss of Documents/Records	M	H	M
Risk 6	Loss of Staff and/or Customers	L	H	H
Risk 7	Transportation	H	M	M

Once you have identified the risk for each, begin to address each in accordance with highest priority. Focus on the most serious risks and most critical functions. It may also be helpful to consider other non-natural risks that could impact your business, such as

Incident/Risk	Likelihood	Preventative Measure	Impact on Business
There is a fire and you are not able to use your site for weeks	Low	Fire resistant equipment, alternative site	Forced to run at 20% of normal activities for a week.
You are burgled and some damage to your property has taken place.	Medium to High	Insurance? Good Security? Separate offsite computer back-up files	Forced to run at 80% of normal activity for a week.
There is a power failure that lasts for days	Low	Backup generator	

3.3 Disaster Mitigation: Because a goal of business continuity planning is to ensure the safety of personnel, customers, and assets during and after a disaster, a critical part of the planning process is to identify the preparedness and preventative measures in place at any point in time. Disaster mitigation techniques include both procedural prevention and physical prevention. Procedural prevention relates to the security and recovery activities performed on a daily basis. Physical prevention and preparedness for disaster include special requirements for building construction, as well as the safety and protection of assets, records, and personnel.

3.4 Identifying Mission Critical Function: The mission critical functions should be identified within all business units and departments. Critical functions include all information, processes, activities, equipment and personnel needed to continue operations should a business unit or department e destroyed or become inaccessible. To determine the mission critical functions of the organization, each department should document all important functions performed within the department. An analysis over a period of two weeks to one month can indicate the principle functions performed inside and outside the department, and assist in identifying the necessary data requirements for the department to conduct its daily operations satisfactorily.

3.5 Outage Impact Analysis: It is important to determine the impact of an outage to the critical systems and business functions. The impact depends on the type of outage that occurs, and the time that lapses before normal operations can be resumed. Other considerations may include the timing of the disaster and the potential impact on the organization (e.g. end-of-month).

3.6 Establishing Priorities: Based on the outage impact analysis, management can establish priorities within business units and departments for the overall recovery of the organization. The business functions can be assigned priorities in the following manner:

a. Essential business functions - a disruption in service exceeding one day would seriously jeopardize the operation of the organization.

b. Important business functions - a disruption of service exceeding one week would seriously jeopardize the operation of the organization.

c. Nonessential business functions - this information would be convenient to have, but would not detract seriously from the operating capabilities if it were missing.

3.7 Testing your IT System: Testing of a business' data backup is a vital process that will determine the correct course of action, as well as point out any flaws in your backup theory.

3.8 Vital Records and Records Disaster Mitigation and Recovery Steps: The management of vital records must be made a part of a business' emergency preparedness responsibility. The identification and protection of records containing information needed to conduct business under emergency operating conditions or protection the legal and financial obligations of a business must be considered.

Include in your business contingency plan a determination of the most critical activities that your business must perform if it must operate under other than normal business conditions and in a facility other than the normal place of business; identify which records support those critical activities and the resumption of normal operations; identify which records series or electronic information systems contain information needed to protect the legal and financial rights of the business and persons directly affected by the business' actions and preserving copies of such records; and establish and implement a plan to recover records that are damaged in an emergency or disaster.

Chapter 4 – Business Continuity

In the aftermath of recent natural disasters, businesses have recognized more than ever the need to be prepared. Companies are striving to meet the demand for continuous service. An organization faces expectations from all sides; customers expect supplies and services to continue in all situations; shareholders expect management control to remain operational through any crisis; employees expect both their lives and livelihoods to be protected; suppliers expect their revenue streams to continue; regulatory agencies expect their requirements to be met; and insurance companies expect due care to be exercised.

Business survival necessitates planning for every type of business disruption including, but not limited to, natural disasters, hardware and communication failures, and failure of supply chain and sales organizations.

Business continuity planning is used to create and validate a practiced plan for how a business or organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption. The well-planned business survives with minimal impact when disaster strikes. Disasters can strike at any time and may take one of several forms individually or collectively – power outages, floods, storms, equipment failure, sabotage, terrorism, and many other factors can contribute to a disruption of normal business operation. Most of us recognize these as possibilities but are you prepared to ride it out with minimal or no loss of data and loss of business revenue and customer goodwill?

Planning makes the critical difference between successfully managing an incident within acceptable parameters and having a situation on hand that may take days, weeks, or months to recover. Risk assessment is the very building block of any contingency plan. Recovery planning and downtime mitigation are largely dependent upon a business facility and its exposures to certain risks. These risks can then be qualified, quantified, and a matrix built upon to begin or enhance a contingency plan. Some facility risks may include, HVAC, electrical, topography of facility, external risks, employees and exposure risks, security, fire risks, facility structure and layout, gas/water lines.

Once you have established what is important to the survival of your business and what the risks are, you can begin to write the plan. A plan should include;

1. A description of what the plan is trying to achieve and how to make it work
2. Essential check lists
3. A description of your premises
4. The structure of the crisis team
5. Emergency provision for staff

1. A description of what the plan is trying to achieve-The plan should focus on the most vital aspects of your business and address the weakest links in your organization.

Things to consider when developing your strategy	Answer
What are the three most vital things to your business?	
What is the weakest link in your business?	
What are the three worst-case scenarios for your business?	
How likely are they to happen?	
What effect will they have on your business?	
What measures can you take to prevent them from happening?	
What measures can you take to minimize the effect they will have on your business?	.

2. Essential Check Lists:

    a. What to do immediately following an incident
    b. What to do after the first hour after the incident
    c. Essential and useful contact details
    d. Essential and useful items
    e. Examples of hardware and software inventory lists that you should have on and off-site

3. Description of your premises:
    a. Location of the emergency exits
    b. Primary meeting point in case of evacuation
    c. Fall-back option if you have to evacuate in a different direction
    d. Details of what the premises contain
    e. Information that is important and specific to your premises i.e. storage facilities

4. The Structure of the Crisis Team: Even though your company is fairly small, you will still find it useful to include information such as when to implement the plan and who has the authority to implement it. Include both senior and junior members of staff in the plan and their respective responsibilities; make sure that there are reserves for each role to cover holidays and sickness.

5. Emergency Provisions for Staff: Think about how your staff will react if quickly evacuated from your building.

Businesses should review their plan and make amendments as needed when key personnel change, who you move to a different location, or when your clients or suppliers change. And make sure you train your staff.

Chapter 5 – Disaster Recovery

The most proactive step a business can take is to have a disaster recovery and business continuity plan in place. The U.S. Department of Labor estimates over 40% of businesses never reopen following a disaster. Of the remaining businesses, at least 25% will close within 2 years. Small businesses who have taken the time to establish a business continuity or disaster recovery plan will be better prepared to rebuild than a business that was ill-prepared.

The key disaster-recovery components that must be in place before the disaster are:

- Backup of data and off-site or online data storage before disasters occur,
- Workable strategies to follow when disaster occur,
- Outline for recovery following the disaster,
- Maintenance of sufficient insurance coverage, and
- Creation of an off-site disaster toolkit that contains all pertinent company information and can be accessed easily upon disaster.

Foremost, following an immediate evacuation or rescue of staff, ambulance transport, family notifications, if necessary, and all staff are accounted for, a previously designated disaster team coordinator will provide a business recovery work area. The disaster coordinator should have available a recovery area checklist and begin to set up emergency business operations. Crucial at this stage is to have planning meetings with all key department personnel and staff to discuss damage assessment, status updates, available resources and business functions, timelines, and assignment of staff. Another function of the disaster coordinator is to make sure that steps are taken as soon as possible to contact the company's insurance providers, the U.S. Small Business Administration, and the Federal Emergency Management Agency.

A disaster recovery plan uses a three-tier approach to self-assessment: 1) recovery, 2) restoration and 3) backup.

5.1 In the backup level,

Data complete and inclusive – a process that ensures critical data files are identified, complete, inclusive and copied to some form of storage media that can be placed in a safe location.

Recovery Point Objective (RPO) – the targeted limit to how old data can be when restored and made available to users.

Recovery Time Objective (RTO) – defines how quickly the system or service must be restored to make available to users.

Off-Site Storage – A separate facility where backup media is stored.

Resources Complete – Having the appropriate recovery environment, staff, software, hardware, supplies, etc. to ensure that a system or service can be recovered.

5.2 In the restoration level,

- Media (tapes, disks, documents) – storage media, which has the data necessary to meet the owner's recovery objectives

- Single Point of Failure – A resource or item that due to its failure or lack of availability leads to an interruption in a business process or causes it to fail entirely.

- Skills – the personnel with the appropriate knowledge of the production environment processes and procedures

- Process – A detailed written explanation of how to perform a specific task related to recovery or operation of a system or service

- Software – computer programs whether "package applications" or custom programs, used as part of a business function to process information stored electronically.

- Hardware – computers and their related peripheral equipment that provide the physical processing, storage and transmissions controls as directed by software to meet the needs of the business function.

Restore includes all of the resources needed to provide functionality. Restoration requires that the broad array of resources needed to support a system or service be considered. Consideration must be given to not only the availability of data, software and hardware, but also the procedures and individuals with the requisite skills to accomplish a recovery. The keys to addressing and effectively maintaining the restore recovery capability are: Regular maintenance to documentation, testing of restore processes, and to the degree appropriate, testing of the end-to-end restore process. Some simple systems may not require a complex environment, but there is still a large quantity of issues.

5.3 In the recovery level,

- Alternate Equipment – technology equipment comparable/compatible with the system production equipment and software that can be used to conduct recovery of a system or service.

- Testing – to exercise a recovery plan and related procedures to verify that the plan and defined resources (equipment, network, data, etc) are adequate to recovery a system or service within targeted timeframes.

- Alternate Location – a site with appropriate power, network, security and space to support the recovery environment for the system or service being recovered.

Recovery can refer to either testing process or the actual response to a disaster. Recovery means that backup data has been restored in a manner that closely simulates recovery from an actual business interruption. It is where the viability of a recovery plan is clearly defined through the success or failure to meet the objectives set by the business owner.

Backup is the most essential component of a recovery capability. Making sure that data, programs, critical documentation are available in the event of a disruption is the most basic requirement. Recovery cannot happen in most cases without careful attention to backup. If Business process owners must re-input data into the system after recovering from a disaster, then written procedures to accomplish the task are a must.

Why plan for disaster recovery and business continuity? Planning procedures can ensure the ability to recover after a disaster. It can also decrease the time to recover. If you had a disaster and it took too long to recover, what would you tell your:

i. Investors
ii. Business partner(s)
iii. Customers
iv. Vendors

Having an understanding of what it means to plan for disaster recovery and business continuity will provide your business with a solid framework from which to create specific plans for your business.

Chapter 9 – Disaster Aid

Once a disaster declaration has been announced, individuals and business owners who have suffered losses may be eligible for assistance.

Nortex Regional Planning Commission has an economic disaster response team available to assist the communities or counties within the Nortex Region to seek assistance. The following is necessary for the Nortex team to assist:

a. Evidence the business was a positive cash flow enterprise. Financial statements are the best means for demonstrating positive cash flow.

b. Insurance papers. All documents that provide information on insurance coverage and amounts.

c. Any information regarding banking transactions.

d. Authorization for the team to access personal information.

Appendix A

BUSINESS CONTINUITY PLAN

Business Name: _____

Address: _____

_____

_____ Cell # _____

Phone #

Emergency Contact Information: Dial 9-1-1 in an Emergency

Non-Emergency: Police: _____

Fire: _____

Insurance Provider: _____

Emergency Planning Team: _____

_____

_____

_____

_____

I. CRITICAL OPERATIONS

The following is a prioritized list of our critical operations, staff and procedures we need to recover from a disaster.

Operation	Staff in Charge	Action Plan

II. SUPPLIERS AND CONTRACTORS

Company Name	**Address, City, State, Zip**	**Phone/Fax/ E-Mail Contact Information**	**Materials/Service Provided**	**If this company experiences a disaster, we will obtain supplies/ materials from the following:**

III. EVACUATION PLAN

Evacuation Plan for:

Name of Company:
Address:
Phone:

- We have developed these plans in collaboration with neighboring businesses and building owners to avoid confusion or gridlock.
- We have located, copied and posted building and site maps.
- Exits are clearly marked.
- We will practice evacuation procedures two times a year.

If we must leave the workplace quickly:

1. Warning System:
2. Assembly Site:
3. Assembly Site Manager and Alternate:
4. Shut Down Manager & Alternate:
5. Person responsible for issuing all clear is _____

Shelter-In-Place Plan for:

Name of Company:
Address:
Phone:

- We have talked to co-workers about which emergency supplies, if any, the company will provide in the shelter location and which supplies individuals might consider keeping in a portable kit personalized for individual needs.
- We have located, copied, and posted building and site maps.
- We will practice shelter procedures two times a year.

If we must take shelter quickly:

1. Warning System:
2. Storm Shelter Location:
3. Shelter Location and Alternate:
4. "Seal the Room" Shelter Location:
5. Shut Down Manager & Alternate:
6. Person responsible for issuing all clear is _____.
7.

Communications:

- We will communicate our emergency plans with co-workers in the following way:

- In the event of a disaster we will communicate with employees in the following way:

Cyber Security:

- To protect our computer hardware, we will _____.
- To protect our computer software, we will _____
- If our computers are destroyed, we will use back-up computers at the following locations:

Records Back-Up:

- Is responsible for backing up our critical records including payroll and accounting systems.
- Back-up reports including a copy of this plan, site maps, insurance policies, bank account records and computer back-ups are stored on-site _____ _____.
- Another set of back-up records is stored at the following off-site location:_____ _____.
- If our accounting and payroll records are destroyed, we will provide for continuity in the following ways:

Employee Emergency Contact Information:

The following is a list of our co-workers and their individual emergency contact information:

Annual Review:

We will review and update this business continuity and disaster plan in _____.

Instructions:

1. Fill in your business name and contact information.
2. Remember: In case of an emergency, always dial 9-1-1. In non-emergency cases, have available phone number and contact information for police, fire, and insurance provider.
3. Make a list of your emergency planning team. For small businesses employing 1-4 employees, or even 5 to 9 employees, this could be one or two people. However, it is important that all employees know who the emergency planning people area.

Section I.

1. List all of your business operations and who is in charge. Identify what procedures will be necessary to recover each operation in the case of a disaster.

Section II.

1. List all of your suppliers and contractors including contact information; the materials or services they provide and alternate suppliers/contractors.

Section III.

1. All businesses should have an evacuation plan with marked exits, maps of exit routes should be posted in the workplace, and a copy of the evacuation plan should be made available to each employee or co-worker. Collaborate with neighboring businesses to avoid confusion. Make sure that all employees or co-workers are aware of the location to assemble in case of disasters.
2. Shelter-in-Place: Emergencies can occur quickly and without warning. It may be necessary to shelter-in-place during disasters. Make sure your disaster supply kit is available and employees or co-workers are aware of the location of these supplies. You should also have a person responsible, or in charge, to issue an "all clear" statement following a disaster.
3. Communicating your emergency plan to all employees or co-workers is vital. You may want to include the plan in your personnel policy, post it in the workplace, or discuss the plan on a regular basis during staff meetings. Whatever means of communication you choose, make sure each employee is aware of the emergency plan. Also, list the manner in which you will communicate with employees during disasters, such as use of cell phones, internet/e-mail service, or other methods.
4. IT security and data recovery procedures – make sure you have critical records backed up and safeguarded. Your server should be located high enough off the floor so that it does not get damaged during a flood. Drivers can be recovered, but they are costly so it is important to have a backup system. Take backup tapes off-site and store in a safe location, such as a safety deposit box. Battery backup and/or surge protection is also important.
5. List each employee or co-worker and their individual emergency contact information.
6. Review and update your emergency plan annually, or more frequently, if you have had changes in staff.

Appendix B
Risk Assessment Guidelines

Here are general guidelines for a Risk Assessment:

1. Establish the risk assessment team. The team will be responsible for the collection, analysis, and reporting of the assessment results to management. It is important that all aspects of the activity workflow be represented on the team, including human resources, administrative processes, automated systems, and physical security.

2. Set the scope of the project. The team should identify the objective of the assessment, the department of function to be assessed, the responsibilities of the member of the team, the standards to be used, and the operations to be observed.

3. Identify assets covered by the assessment. Assets may include personnel, hardware, software, data, facilities, and current controls that safeguard those assets.

4. Categorize potential losses. Identify the losses that could result from any type of damage to an asset, such as physical damage, denial of service, modification, etc.

5. Identify threats and vulnerabilities. Threats could be natural threats, accidental threats, or human accidental or malicious threats. This could include power failure, hazardous chemical spills, acts of nature, or hardware/software failure. Vulnerabilities are weaknesses which a threat will result in attacking your assets. This could include system security, policies and procedures, management, etc.

6. Identify existing controls. Controls are the safeguards that reduce the probability of a threat damaging or destroying your business.

7. Analyze the data. Collected information can be used to determine the actual risks to your assets. A technique to analyze data includes preparing a list of assets and showing corresponding threats, type of loss, and vulnerability. Analysis of this data should include an assessment of the possible frequency of the potential loss.

8. Determine cost-effective safeguards. Include in this assessment the implementation cost of the safeguard, the annual cost to operate the safeguard, and the life cycle of the safeguard.

9. Report. Prepare a simple report that is easy to read, and supported by detailed analysis. This type of report is more easily understood by individuals who may not be familiar with your organization. The report should include findings, such as a list

of assets, threats, and vulnerabilities; a risk determination, recommended safeguards, and a cost benefit analysis.

APPENDIX C
DISASTER RECOVERY PLAN

Section 1. Goals of a Disaster Recovery Plan

The major goals of a disaster recovery plan are:

- To minimize interruptions to normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train network engineers and managers on emergency procedures.
- To provide for smooth and rapid restoration of service.
- Establishing high WAN/Internet connection reliability and fault tolerance.
- The following is a list of all IT personnel who are involved with information technology aspects. This list should be updated frequently.

Section 2. Personnel

Data Processing Personnel			
Name	**Position**	**Address**	**Telephone**

Section 3. Application Profile

This is a list of all application personnel who are involved with payroll, accounts payable/receivable, orders, etc.

Application Profile				
Application Name	**Critical? Yes or No**	**Fixed Asset? Yes or No**	**Manufacturer**	**Comments**

Comment Legend:

1. Runs Daily
2. Runs Weekly On
3. Runs Monthly On

Section 4. Inventory Profile

This is a list of physical inventory that involves your LAN & WAN. This list should be updated frequently and should include all components to your network. This list should include the following:

- Processing units
- Disk units
- Models
- Workstation Controllers
- Personal Computers
- Spare Workstations
- Telephones
- Air Conditioner or Heater
- System Printer
- Tape and Diskette Units
- Controllers
- I/O Processors
- General Data Communication
- Spare Displays
- Racks Humidifier or Dehumidifier Power Generator?

Inventory Profile					
Manufacturer	**Description**	**Model**	**Serial Number**	**Own or Leased**	**Cost**

NOTE: This list should be audited every _____ months.

Miscellaneous Inventory		
Description	**Quantity**	**Comments**

Note: This list should include the following:

- Tapes
- PC software
- File cabinet contents or documentation
- Tape vault contents

- Diskettes
- Emulation Packages
- Language Software
- Printer Supplies

Section 5. Information Services Backup Procedures

This procedure saves the journals and journal receivers.

- On _____ (day) at _ (time) a complete save of the system is done.

- All saved media is stored off-site in a vault at _____ (location) or in an on-line storage site: _____.

- Personal Computer

- It is recommended that all personal computers be backed up. Copies of the personal computer files should be uploaded to the server on _____ _____ (date) at _____ (time), just before a complete save of the system is done. It is then saved with the normal system save procedure. This provides for a more secure backup of personal computer-related systems where a local area disaster could wipe out important personal computer systems.

Section 6. Disaster Recovery Procedures

For any disaster recovery plan, the following three elements should be addressed:

- Emergency Response Procedures: To document the appropriate emergency response to a fire, natural disaster, or any other activity in order to protect lives and limit damage.

- Backup Operations Procedures: To ensure that essential data processing operational tasks can be conducted after the disruption.

- Recovery Actions Procedures: To facilitate the rapid restoration of a data processing system following a disaster.

Section 7. Recovery Plan-Mobile Site

1. Notify _____ of the nature of the disaster and the need to select the mobile site plan.
2. Confirm in writing the substance of the telephone notification to _____ within 48 hours of the telephone notification.
3. Confirm all needed backup media are available to load the backup machine.
4. Prepare a purchase order to cover the use of backup equipment.

5. Notify _____ of plans for a trailer and its placement on _____.
6. Depending on communication needs, notify telephone company _____ of possible emergency line changes.
7. Begin setting up power and communications at _____.
    a. Power and communications are prearranged to hook into when trailer arrives.
    b. At the point where telephone lines come into the building _____ break the current linkage to the administration controllers ____. These lines are rerouted to lines going to the mobile site. They are linked to modems at the mobile site. The lines currently going from _____ to _____ would then be linked to the mobile unit via modems.
    c. This could conceivably require _____ to redirect lines at ___ complex to a more secure area in case of disaster.
8. When the trailer arrives, plug into power and do necessary checks.
9. Plug into the communications lines and do necessary checks.
10. Begin loading system from backups.
11. Begin normal operations as soon as possible:
    a. Daily Jobs
    b. Daily Saves
    c. Weekly Saves
12. Plan a schedule to back up the system in order to restore on a home-base computer when a site is available. (Use regular system backup procedures.)
13. Secure mobile site and distribute keys as required.
14. Keep a maintenance log on mobile equipment.

Section 8. Recovery Plan-Hot Site

The disaster recovery service provides an alternate hot site. The site has a backup system for temporary use while the home site is being reestablished.

1. Notify _____ of the nature of the disaster and of its desire for a hot site.
2. Request air shipment of modems to _____ for communications.
3. Confirm in writing the telephone notification to _____ _____ within 48 hours of the telephone notification.
4. Begin making necessary travel arrangements to the site for the operations team.
5. Confirm that all needed tapes are available and packed for shipment to restore on the backup system.
6. Prepare a purchase order to cover the use of the backup system.
7. Review the checklist for all necessary materials before departing to the hot site.
8. Make sure that the disaster recovery team at the disaster site has the necessary information to begin restoring the site.

9. Provide for travel expenses (cash advance).
10. After arriving at the hot site, contact home base to establish communications procedures.
11. Review materials brought to the hot site for completeness.
12. Begin loading the system from the saved tapes.
13. Begin normal operations as soon as possible.
14. Plan the schedule to back up the hot-site system in order to restore on the homebased computer.

Section 9. Restoring the Entire System

To get your system back to the way it was before the disaster, use the procedures on recovering after a complete system loss in the Backup and Recovery sections.

Before You Begin: Find the following tapes, equipment, and information from the on-site tape vault or the off-site storage location:

- If you install from the alternate installation device, you need both your tape media and the CD-ROM media containing the Licensed Internal Code.
- All tapes from the most recent complete save operation
- The most recent tapes from saving your configuration, if necessary
- All tapes from the most recent daily save operation
- Tape list from most recent complete, weekly, and daily save operations
- History log from the most recent complete, weekly, and daily save operations
- The Software Installation Book
- The Backup and Recovery Book
- Telephone directory
- Modem manual
- Tool Kit

Section 10. Rebuilding Process

The management team must assess the damage and begin the reconstruction of a new data center. If the original site must be restored or replaced, the following are some of the factors to consider:

- What is the projected availability of all needed computer equipment?
- Will it be more effective and efficient to upgrade the computer systems with newer equipment?
- What is the estimated time needed for repairs or construction of the data site?
- Is there an alternative site that more readily could be upgraded for computer purposes?

Section 11. Testing the Disaster Recovery Plan

In successful contingency planning, it is important to test and evaluate the plan regularly. Data processing operations are volatile in nature, resulting in frequent changes to equipment, programs, and documentation. These actions make it critical to consider the plan as a changing document. Use this checklist as you conduct your test and decide what areas should be tested:

Conducting a Recovery Test:

Item	Yes	No	Applicable	Not Applicable	Comments
Select the purpose of the test. What aspects of the plan are being evaluated?					
Describe the objectives of the test. How will you measure successful achievement of the objectives?					
Meet with management and explain the test and objectives.					
Have management announce the test and the expected completion time.					
Collect test results at the end of the test period.					
Evaluate results. Was recovery successful? Why or Why Not?					
Determine the implications of the tests results. Does successful recovery in a simple case imply successful recovery for all critical jobs in the tolerable outage period?					

Make recommendations for changes. Call for responses by a given date.					
Notify other areas of results. Include users and auditors.					
Change the disaster recovery plan manual as necessary.					

Areas to be tested:

Item	Yes	No	Applicable	Not Applicable	Comments
Recovery of individual application systems by using files and documentation stored off-site.					
Reloading of system tapes and performing an IPL by using files and documentation stored offsite.					
Ability to process on a different computer.					
Ability of management to determine priority of systems with limited processing.					
Ability to recover and process successfully without key people.					
Ability of the plan to clarify areas of responsibility and the chain of command.					

Effectiveness of security measures and security bypass procedures during the recovery period.					
Ability to accomplish emergency evacuation and basic first-aid responses.					
Ability of users of real-time systems to cope with a temporary loss of on-line information.					
Ability of users to continue day to-day operations without applications or jobs that are considered not critical.					
Ability to contact the key people or their designated alternates quickly.					
Ability of data entry personnel to provide the input to critical systems by using alternate sites and different input media.					
Availability of peripheral equipment and processing, such as printers and scanners.					
Availability of support equipment, such as air conditioners and dehumidifiers.					
Availability of support: Supplies, transportation, and communication.					
Distribution of output produced at the recovery site.					
Availability of important forms and paper stock.					
Ability to adapt plan to lessen disasters.					

Section 12. Disaster Site Rebuilding

- Floor Plan of Data Center
- Determine current hardware needs and possible alternatives. (See Section 4. Inventory Profile) ○ Data center square footage, power requirements and security requirements.
    - Square Footage:_____
    - Power Requirements:_____.
    - Security Requirements: Locked area, preferably with combination lock on one door.
    - Floor-to-ceiling studding ○ Detectors for high temperature, water, smoke, fire and motion ○ Raised floor

Floor Plan (Include a copy of the proposed floor plan here.)

Section 13. Record of Plan Changes

Keep your plan current. Keep records of changes to your configuration, your applications, and your backup schedules and procedures.

Vendors – Include Vendor Information Here			
Company Name	**Contact**	**Address**	**Telephone**

Appendix D
Self-Assessment

DISASTER ACTION CHECKLIST:

1. **Plan Initiation:**

   Notify Senior Management

   Contact and Setup the Disaster Recovery Team

- Determine Degree of Disaster
- Implement Proper Application Recovery Plan dependent on extent of disaster
- Monitor Progress
- Contact Backup Site and Establish Schedules
- Contact all Other Necessary Personnel – both user and data processing
- Contact Vendors – both hardware and software
- Notify Users of the Disruption of Service

2. Follow-up Checklist:

- List Teams and Tasks of Each Person
- Obtain Emergency Cash and Setup Transportation To and From the Backup Site
- Setup Living Quarters, if necessary
- Setup Eating Establishments, as required
- List All Personnel and Their Telephone Numbers
- Establish User Participation Plan
- Setup the Delivery and the Receipt of Mail
- Establish Emergency Office Supplies
- Rent or Purchase Equipment, as needed
- Determine Applications to be Run and in What Sequence
- Identify Number of Workstations Needed
- Check Out Any Off-Line Equipment Needs for Each Application

- Check on Forms Needed for Each Application
- Check All Data Being Taken to the Backup Site before Leaving and Leave an Inventory Profile at a Home Location
- Setup Primary Vendors for Assistance with Problems Incurred During Emergency
- Plan for Transportation of Any Additional Items Needed at the Backup Site
- Take Directions (Map) to Backup Site
- Check for Additional Magnetic Tapes, if required
- Take Copies of System and Operational Documentation and Procedural Manuals.
- Ensure That All Personnel Involved Know Their Tasks
- Notify Insurance Companies

Management			
Name	**Position**	**Address**	**Telephone**

Recovery Start-Up Procedures For use After a Disaster

1. Notify _____ Disaster Recovery Services of the need to utilize service and of recovery plan selection. NOTE: Guaranteed delivery time countdown begins at the time is notified of recovery plan selection. Disaster Notification Numbers _____ or_____. These telephone numbers are in service from ___a.m. until ___ p.m. Monday through Friday.
2. Disaster Notification Number:___ This telephone number is in service for disaster notification after business hours, on weekends, and during holidays. Please use this number only for the notification of the actual disaster.
3. Provide _____ with an equipment delivery site address (when applicable), a contact, and an alternate contract for coordinating service and telephone numbers at which contacts can be reached 24 hours a day.
4. Contact power and telephone service suppliers and schedule any necessary service connections.
5. Notify _____immediately if any related plans should change.
6. Contact Nortex Regional Planning Commission's Economic Disaster Response Team.