

Disaster Planning and Recovery

*An Agency's Guide to
Building a Disaster Plan*



Table of Contents

Introduction

The Constant Threat of Disaster.....	4
The Purpose	6

Section 1: Develop Your Own Disaster Plan

Establishing a Planning Team	7
Assessment of Potential Disasters and Organizational Capabilities.....	8
<i>A. Potential Disasters</i>	8
<i>B. Organizational Capabilities</i>	8
Writing Your Own Disaster Plan	9
<i>A. Body of the Disaster Plan</i>	9
• Recovery Teams Chart	11
• Preparations Chart.....	12
<i>B. Appendices</i>	13
Distribute the Plan.....	14
Test the Plan	14
Plan Evaluation and Modification.....	14
“A Special Look at I.T.: Is Your System Ready for Fallout?”.....	15

Section II: Recovery After the Disaster

Remember, Safety First!.....	16
Consider a Back-Up Facility.....	16
Communication is the Key.....	16
<i>A. Disaster Recovery Teams</i>	17
<i>B. Customer Relations</i>	17
<i>C. Company Relations</i>	17
<i>D. Employee Relations</i>	17

Section III: Informational Resources

Ready.gov Sample Business Continuity and Disaster Preparedness Plan.....	20
Employee Contact Information List.....	27
Building Your Disaster Plan: A Checklist for Existing Controls.....	28
Saffir-Simpson Hurricane Scale.....	47
Statewide Evacuation Routes Map.....	48
Back-Up Facility Supply Kit.....	49
Important Telephone Numbers.....	50
Disaster Recovery Log Template.....	51
FSLSO Catastrophe Information Form.....	52

Disaster Planning and Recovery: An Agency's Guide to Building a Disaster Plan was created by the Florida Surplus Lines Service Office. The approaches presented in this guide are only recommendations, not regulations. Following these suggested guidelines will not ensure compliance with any Federal, State or local codes or regulations. The principles used in this manual should be used as suggestions only.

The FSLSO was created by the Florida Legislature as a self-regulating, not-for-profit association to protect consumers and state revenues by facilitating industry compliance and serving as a source of information and advice concerning the surplus lines insurance marketplace in the state of Florida.



Introduction

Disasters can occur with little notice for preparation. A majority of preparation work can be done far in advanced through the development of disaster plan. The 2004 Hurricane Season raised the bar for disaster preparedness – prepare for the worst and hope for the best. In light of the 2004 hurricane season, the FSLSO has developed a catastrophe manual that can aid an agency in developing a specialized disaster plan.

The Constant Threat of Disaster

For most, the most commonly associated natural catastrophe that impacts the sunshine state is the seasonal threat of hurricanes. As each yearly hurricane season draws to a close, we are freshly reminded of the devastation that can occur from the impact of a single storm.

Few Floridians will quickly forget the massive destruction that resulted from Hurricane Andrew on August 24, 1992. What began as a small yet fierce Cape Verde hurricane became the third strongest hurricane to ever impact the United States. Andrew hit the sunshine state with sustained winds ranging between 145-175 mph, and continued to strengthen with isolated wind gusts estimated at more than 200 mph.

Andrew struck southern Dade County with violent winds and storm surges characteristic of a Category 5 hurricane on the Saffir-Simpson Hurricane Scale. In Dade County alone, there were 15 casualties and a quarter of a million people were left temporarily homeless.

While the death toll for Andrew remained substantially low for a hurricane of its force (combined direct and indirect casualties from Andrew totaled 61), the associated cost soared to

an estimated \$27 billion in total losses, making it the costliest hurricane in United States history at the time. Had Andrew come only 20 miles more northerly, the financial and casualty impact would have been significantly higher.

In the wake of Andrew's aftermath, Floridians filed more than 600,000 claims and insurance companies paid out nearly \$16 billion.



Efforts to prevent such massive structural damage from a natural disaster have resulted in revamped building codes and structural construction. These efforts played a huge role in 2004, as Florida, once again, faced a devastating hurricane season.

Within a 45 day-period beginning August 13, the state of Florida was hit with a total of four hurricanes. The procession of destructive storms left thousands of Floridians homeless. Charley was followed by Hurricane Frances, which came ashore on September 5 with 105 mph winds at Sewall's Point.

Hurricane Ivan proved to be the season's mammoth storm. With winds that reached 165 miles an hour, Ivan was one of the strongest hurricanes in recorded history. It weakened considerably before its eye finally came ashore near Mobile Bay, Alabama, on September 16. The

storm's front right quadrant, which housed the strongest winds and largest storm surge, smashed into Pensacola, Florida.

Hurricane Jeanne, with winds of 115 mph made landfall on September 25 at nearly the exact same spot as Hurricane Frances. Governor Jeb Bush issued orders declaring a state of emergency during the 45-day time period and President George W. Bush declared most of Florida a federal disaster area.

The 2005 Hurricane Season shattered all records for most named storms in a single season with 27 named storms. Meteorologists were forced to use the greek alphabet to name the last five storms of the season after forecasters exhausted the standard lists of names.

The most notable storm of 2005, Katrina, whose initial readings placed it among the most intense storms since 1900, cut a wide swath of destruction across the Gulf Coast states of Louisiana, Mississippi and Alabama.

Two months after Katrina hit the Gulf Coast,

the death toll stood at 1,289. Thousands were displaced to shelters around the country as entire communities and cities were flattened by the storm

According to the AIR Tropical Cyclone Model, four or more hurricanes are expected to make U.S. landfall in a single season once in every 12 years, while three or more hurricanes will likely make landfall in Florida about once every 40 years.



In addition to the annual threat of the hurricane season, there are a variety of other natural disasters that threaten the state of Florida. The ever growing presence of floods, tornadoes, and forest fires remain constant perils year round.

Along with weather threats, the attacks on the World Trade Center and the Pentagon on September 11, 2001 proved that the devastating impact of terrorism on the United States was yet another force to be reckoned with. The terrorist attacks of September 11 produced the single largest insurance loss in world history -- spanning many lines of coverage including property, life, liability aviation, and workers compensation and resulting in a total loss

2005 Statistics

By the Numbers:

Seasonal average

Named storms: 10

Hurricanes: 6

Major hurricanes: 2

2005 season

Named storms: 27

Hurricanes: 13

Major hurricanes: 7

☞ Three of the hurricanes in the 2005 season reached Category 5 status, meaning they had wind speeds greater than 155 mph at some point during the arc of the storm.

☞ According to FEMA, insurance claims totaled some \$23 billion. Reconstruction costs were estimated to be at least \$200 billion, making Katrina the costliest storm in history.

of more than \$40 billion.

The Purpose

Being prepared is the best defense in light of a disaster. This guide provides step-by-step advice on the creation and maintenance of your organization's disaster plan. Regardless of the type or size of your organization, having a plan ready will directly affect the success or failure of your business.

This manual provides a basic understanding to help Florida's surplus lines agents develop their own Disaster Preparation and Recovery (DPR) plan. The sections below include:

I. Developing Your Disaster Plan: Building your planning team, analysis of potential disasters in your area and structural analysis/maintenance. Also included is a final checklist of items to take care of before leaving your office in the wake of a disaster.

II. Recovering After the Disaster: How to handle your customers, claims, and the recovery of your organization's daily functions.

III. Informational Resources: Includes a variety of resources, phone and fax numbers and disaster checklists.

DEVELOP YOUR OWN DISASTER PLAN. The following information provides a basic outline of items that should be addressed in your disaster plan. A disaster plan should be customized to fit the needs and resources of your office and the following information should be used as a basic guide for the creation of your own disaster plan.

Getting Started

While creating a Disaster Plan may seem overwhelming, the process can be easily broken down into smaller sections, tackling each one at a time, in a defined and logical order. You should begin by creating a written emergency preparedness policy statement, defining the purpose and scope of your plan.

The Planning Team

When establishing your planning team, you will need to include participants from your organization's vital functional areas including:

- Upper Management
- Human Resources
- Information and Technology
- Customer Service
- Finance
- Communications/ Media Relations

Define organizational structure, with a defined chain of command, staff roles and responsibilities.

Appoint a Disaster Plan Coordinator (this individual will be in charge of putting the plan together and maintaining all documentation and audits).

You should also organize the Disaster Planning

Team with proper alternates and back-up members.

Once the Disaster Planning Team has been selected, you are ready to begin drafting your plan.

Assessment of Potential Disasters and Organizational Capabilities

During the initial planning stages of disaster plan building, the team should make a general assessment of the most likely disaster scenarios. As mentioned in the introduction, the types of disaster scenarios have changed dramatically over the past decade. While naturally occurring incidences such as hurricanes, tornadoes, earthquakes, fires, and flood are some of the more common situations, we are now faced with other threats such as blackouts, computer viruses and terrorism.

The impact of different scenarios on an organization serve as a vital component for building an organization's disaster plan. Floods and fires have higher tendencies to incur facility losses including equipment and informational assets but a significantly lower potential for employee loss. Hurricanes, tornadoes, and earthquakes may impact equipment, informational resources, facility and employees.

You should also analyze the physical vulnerability of your facility including the internal and external structure. You may want to consider multiple perspectives in order to analyze the disaster risk that could affect your organization. Consider the following:

A. Potential Disasters

<i>Perspective Areas</i>	<i>Questions to Consider</i>
Historical	<i>What types of potential risks/emergencies have occurred in your organizations area in the past?</i>
Geographical	<p><i>What types of past risks/emergencies have resulted based on your facility's location?</i></p> <ul style="list-style-type: none"> • These may include flood zones, proximity to businesses that carry potential hazardous materials, coastline regions that could be susceptible to storm surge or hurricane.
Technological	<p><i>What could result from a failure from an internal system?</i></p> <ul style="list-style-type: none"> • Such failures could include computer failure/database loss, heating/cooling malfunction (particularly in rooms that may be temperature controlled for electrical equipment use, telecommunication failure, and fire/explosion.)
Human Error	<i>What types of situations or emergencies may result from human error? Are employees properly trained in your organization's workplace safety procedures?</i>
Physical	<p><i>What types of risks/emergencies can be related to the design and/or construction of your organization's physical structure?</i></p> <ul style="list-style-type: none"> • Assess the physical characteristics of your organizations facility and identify the most vulnerable areas. In an emergency in which building preparations can be made, identify the steps that would be necessary to minimize damage. • Identify the types of damage that could accompany a variety of disasters including loss of electrical power, broken gas mains, water damage, smoke damage, and structural damage.

B. Organizational Capabilities

Planning and development of the disaster plan should also incorporate the identification of key products, services and operations that could be affected in a disaster situation. This information will allow you to assess the impact that a potential disaster could have and will allow you to establish procedures for each of these factors.

Areas that may need a review include:

- ↳ the facilities and equipment used to produce company products and services;
- ↳ services or products that are provided through the utilization of a vendor or supplier;
- ↳ operational services including water, power, gas, sewer, telecommunications, transportation and food
- ↳ operational equipment necessary for

continued organizational functions including personnel.

Finally, assess the potential impact that a disaster will have on your organization's daily functions and the impact that it will also have on your customers. How will you manage your customers following an emergency/disaster?

You should consider the potential impact of damages or property loss that could affect your organization. These factors should include costs to repair or replace damaged equipment or the capabilities of setting up a temporary back-up facility.

Writing Your Own Disaster Plan

Now that your organization has completed an impact/risk assessment, it is time for the Disaster Planning Team to begin work on a Disaster Plan.

Your organization's Disaster Plan should incorporate all preparatory items that must be taken care of prior to the arrival of a disaster and

Are You Ready?

Writing your own disaster plan should be thorough, but doesn't have to be complicated. A variety of organizations can provide assistance through existing forms and templates that offer good starting points for the development of your plan.

The U.S. Department of Homeland Security at www.ready.gov provides a multitude of disaster planning guides and applicable forms. Section III of this manual provides one of their basic templates for the building of a disaster preparedness plan.

what must be done in the wake a disaster.

The Planning Team should also outline a basic Plan of Action. The Plan of Action should establish policies and procedures to:

- Activate an Emergency Command Center (if applicable)
- Receive and process emergency calls and information
- Alert and warn personnel
- Engage in disaster preparations as outlined in the Disaster Plan (please see 48 Hours Before the Storm on page 12 for an example)

Your disaster plan should be catered for the size and resources of your particular organization. Your disaster plan should also be in

writing – a plan not in writing is no plan at all.

The following information can be used as a basic guide for the creation of your own disaster plan. In this manual, we have broken down a Disaster Plan into two parts: The Body and the Appendices.

A. Body of the Disaster Plan

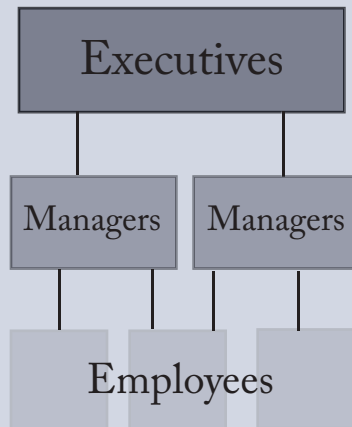
Your disaster plan has several major components:

Emergency information sheet: One-page summary of immediate steps to be taken and individuals to be contacted.

Introduction to the plan: Its purpose, author, organization, and scheduled updates.

Communication plan (or "telephone tree"): Names of staff and others to be contacted, including home, mobile and emergency numbers, strategy for contacting them, and communication vehicles that can be used. Keep in mind that if your area suffers from power loss, electronic phones will not be operable – a back-up phone

Telephone Tree



A telephone tree is an effective method for communicating information down the chain of command.

This basic system provides a simple, but accessible method for an organization to review the status of its employees and remains organized.

system may be necessary to have in place.

Recovery team members: List of recovery team members (including work and home phone numbers), with description of their responsibilities, scope of authority, and reporting lines. Though the size of your organization may determine the number and types of teams you have, consider the chart on the following page.

Important Documents: Have all important documentation, including all items of priority that must

be kept secure and salvagable, listed out by order of importance, locations by department and the name of staffers responsible for their collection as part of your salvage operations.

Prevention/Protection strategy: Schedules, procedures, and persons responsible for routine testing and inspections (e.g. fire alarms and suppression systems, roof, etc.), for follow-up on reported problems, and for ensuring you are properly insured and that insurance records and claims information is explained and accessible.

Insurance Protection: Insurance can cover the cost of replacing or repairing equipment or facilities damaged by some disasters. Optional business interruption insurance can protect you

from extra expenses incurred during the recovery period. Regardless of what type of insurance an organization has, it must be consistent with the provisions of your disaster plan. Having a well documented and continually tested disaster plan can help reduce your insurance premiums.

Typical coverage that should be considered include:

- *Data Processing Property Protection Coverage*
- *Insurance on Computer Hardware*
- *Insurance on Other Data Processing and Office Equipment*
- *Business-Interruption Insurance*

A detailed list of all insurance policy information (including policy number, company, contact phone numbers, etc.) should be included.

Education/Assistance strategy: Outline procedures for providing customers and retail agents with emergency contact information and educate the retail agent with a list of their responsibilities to the policyholder and include who is responsible for providing up-to-date emergency contact information to the FLSO.

Accounting information: Description of institution funds available in a recovery effort and procedures/authorization for access to them.

Insurance information: Explanations of coverage, claim procedures, record-keeping requirements, restrictions on staff/volunteers entering a disaster area, information on state/federal disaster relief procedures.

Checklist of pre-disaster actions: Outline of procedures to be followed in advance of an emergency for which there is advanced warning (e.g. hurricane, flooding), including assignment of responsibilities for those actions, communication networks and back-up facilities.

Procedures for your pre-disaster checklist should include routine preparation procedures that

<i>Team</i>	<i>Responsibilities</i>
Emergency Management Team	Composed of senior management and supervisors; oversees the operations of response and recovery and makes adjustments as needed.
Call Team	Responsible for manning the phone lines and taking all incoming phone calls from clients.
Personnel Team	Responsible for taking care of clients that walk through the door. Walk-ins should be taken to a designated area where their concerns can be handled and the claims process can be started.
Processing Team	Responsible for getting all of the customer's claim information down on paper and having it processed.
Filing Team	Responsible for pulling and replacing files; members of this team may also be used as a "courier" service, moving files/items to and from the office.
Special Projects Team	Responsible for transportation of staff to and from facility (if needed), acquisition of necessary supplies, materials, and equipment.
Finance and Accounting Team	Responsible for managing all transaction of funds and records (cash, credit card, with corresponding receipts), division of petty cash monies and all money records.
Information Technology Team	Responsible for assessing damages done to any computer systems, obtaining recovery tapes (back-up tapes), and recovery of critical systems for production processes.
Media	Responsible for dealing with all media outlets. It may also serve as a useful tool, particularly for a larger agency, to have a media packet together with all emergency numbers and instructions listed so as to educate the public of their responsibilities in order to get the claims process started. These packets may be distributed as needed based on the severity of a disaster and should be kept up-to-date as part of the disaster plan.

Instructions for response and recovery:

Routine Preparations	48 Hours Before	24 Hours Before
<p>1. All electronic files should be saved and “backed-up” on a daily basis.</p> <p>2. Remove or isolate flammable materials. Clearly mark gas and water shut-off valves and fuse box. Post legible instructions on how to shut off each one.</p> <p>3. Maintain a conveniently located set of tools to facilitate prompt gas shut off (including pipe or crescent wrenches).</p> <p>4. Post locations of water and gas shut-off valves and fuse box in central locations.</p> <p>5. Place a facility evacuation plan in an area accessible to office staff.</p> <p>6. Make sure your workplace disaster supply kit is up-to-date:</p> <ul style="list-style-type: none"> • <i>Portable radio and extra batteries</i> • <i>Emergency first aid supplies</i> • <i>Flashlight and extra batteries</i> • <i>Wrenches and other tools</i> • <i>Fire extinguishers</i> • <i>Food and water for employees/customers for a period of unexpected confinement</i> 	<p>Debrief the Staff: Establish a meeting in which all staff members can participate. Make sure that everyone is familiar with your organizations emergency procedures and are aware of their own responsibilities for both pre-disaster preparation and aftermath recovery.</p> <p>Back-Up Computer Data: Even if your organization’s procedures call for daily back-ups, make sure that all backed-up information is safely stored off the premises. This may be your last opportunity to get electronic data safely out of your building and deposited to a safer location.</p> <p>Generate Paper Documentation: Double-check your supply of claim forms to make sure that you have enough in stock. If you are running in short supply, this may be one of the last opportunities to make extra copies.</p> <p>Back-Up Facility Supplies: Allocate all items that will need to go to your back-up facility. The closer an impending storm gets to your area, the fewer supplies will be available. See page 49 in the Informational Resources Section for a sample list of back-up facility supplies.</p>	<p>Evacuation: Identify evacuation requirements for your area. If necessary, determine who on your staff is evacuating, how they can be contacted, how far away they are going, and when they will be coming back. You will need to know who will be available to work following the storm and what their responsibilities are for organizational recovery – what kind of impact will missing staff have on the recuperation and daily operations of the organization following the storm?</p> <p>Draft Authority: Contact your insurance companies requesting draft authority in light of an oncoming storm. If you are given authority, you will be able to better serve your customers in expediting their claims process.</p> <p>Office Preparation: Complete preparatory steps that will minimize facility damage (may include putting up plywood or preparing sandbags.)</p> <p>Equipment: Move equipment, furniture, records, and supplies to a safe area of the office (elevate items that may be threatened by flooding and move all materials away from windows) or to an off-site premises. Cover office furniture, filing cabinets, furniture with protective, plastic covering. <u>Unplug all electrical equipment.</u></p>

should be completed 48 hours before an oncoming disaster (if a disaster merits preparatory time); and procedures that should be completed within 24 hours of a disaster's approach.

Internal Instructions: Detailed, step-by-step instructions on all phases of salvage operation, including discussion of recovery from the range of incidents that are possible (e.g. roof/plumbing leaks, flooding, fire, etc.) and covering the various media (paper and electronic documentation).

Also include procedures for handling policyholder claims and interacting with state and federal regulators, i.e., if you will be adjusting claims, contact the insurer to secure check writing authority if insurer is agreeable. Also, have access to available claims reporting information, i.e. requests from the DFS/OIR to provide claims information to their offices.

External Instructions: Detailed, step-by-step instructions on all phases of customer claims handling procedures, communications with retail agents and regulators, and plans for long-term recovery.²

B. Appendices

The Appendices section of your disaster plan should include any charts, lists or information resources that accompany your disaster plan. Other informational resources may also include form templates, detailed building schematics/drawings, evacuation routes/instructions and floor plans.

Documentation priorities within departments, locations: Lists that include names of staff for each area, and location (perhaps indicate a floor plan).

Checklist for prevention/protection inspections: Extra copies of forms to be used.

Record-Keeping forms: Multiple copies of all forms that may be needed in the salvage

operation, including inventory forms, packing lists, requisitions and purchase orders, etc.

Detailed building plans: Separate sets covering each of the following: storage areas, aisles, entrances and exists, windows, fire extinguishers, fire alarms, sprinklers, smoke/fire detectors, annunciates, shut-offs and master switches for power, water, gas, HVAC (heating, ventilation, and air-conditioning) system, elevator controls, etc.

Resource lists: Locations and inventory of in-house supplies, sources of commercial supplies/equipment that may be purchased, names of consultants and other specialists, sources of auxiliary/volunteer personnel, etc. For lists of resources outside the institution, it will be useful to provide day and night/weekend contacts and phone numbers, along with some details about the resources such as the type and quantities of materials available, cost and payment terms, and/or special arrangements/contracts that exist.

Location of keys: Information about the location of and means of access to keys or combinations for special collections, elevators, offices, etc. Note: For security reasons, it may not be prudent to

Back It Up!

Even with daily backing up of data, also consider the following questions:

1. Is the back-up data stored offsite?
2. Is there more than one person with access to the backup data?
3. Has a successful recovery of the backup data ever been tested?
4. Does the business have immediate access to a computer to recover the data?
5. Is the backup system tested after each major upgrade of the system?

8

provide exact information about all of these. In such cases, the plan should specify a procedure for contacting the individuals who have the proprietary information.

Off-Site Vital Records List: You should maintain a list of the types of files (by company or subject) that are stored off-site. As some records may be confidential, you will want to make sure they are accounted for and not lost in a move.

Distribute the Plan

How you choose to bind your Disaster Recovery Plan is up to your discretion. An inexpensive way to bind your plan is with a three-ring binder, with a front cover design that should include the organization's name/logo and the document title. Determine which individuals within your organization should receive a copy of the plan and consider the following list:

- 1) Chief Executive and Senior Management
- 2) Key members of the organization's emergency response team
- 3) Organization's headquarters if located in another region
- 4) Key personnel members should keep a copy in their homes

Staff members should have an opportunity to familiarize themselves with the plan and training may be required.

Test the Plan

Staff members should have a basic understanding of:

- ☞ *Individual roles and responsibilities;*
- ☞ *The organizations emergency procedures;*
- ☞ *Location of common use emergency equipment;*
- ☞ *Emergency shutdown procedures.*

There are a variety of methods in which you can test your plan: tabletop exercises, walk-through

drills, evacuation drills and full-scale "mock disaster" exercises are methods in which you can put your plan to the test. Testing of your plan should be done at least once a year.

Plan Evaluation and Modification

Routine evaluation of an organization's disaster plan will allow for modifications to be made to the existing plan. An annual audit of an organizations' disaster plan will generally suffice, unless other measures with a significant impact arise throughout the year.

During an annual evaluation, consider the following points:

- ☞ *Are all problems or shortfalls identified during the vulnerability analysis being dealt with sufficiently?*
- ☞ *Does the plan reflect lessons learned from previous events?*
- ☞ *Do all staff members understand their responsibilities and roles as dictated by the Plan?*
- ☞ *Does the Plan reflect any physical changes to the building facility? Does it reflect new or different procedures/processes?*

☞ *Are the names, titles, and telephone numbers current?*

Along with an annual examination, an organization's disaster plan should be evaluated and modified following training drills, real-life emergencies, changes in personnel, alterations to facility, or process/procedural changes.

Additional Training

The organization may also seek additional training for management and staff employees after the initial distribution of the Plan.

Training exercises and activities can include a variety of options including routine fire drills, educational classes, and walk-through drills.



A Special Look at Information Technology: Is Your System Ready for Fallout?

In the case of electronic information resources, there are special considerations and some of these are not obvious. System data backups do not ensure successful recovery from a disaster; to understand this point, address the following questions:

Is all electronic documentation and data being backed up on a regular basis?

While backing up servers and shared file storage is a common approach to routine maintenance, it may not serve as a complete back-up system – do not neglect employee workstation computers, laptops or mobile devices.

How easily can physical hardware be replaced if necessary? Where can it be obtained and how long will it take?

Any part of your I.T. system can fail – in the best case scenario, redundant components will automatically compensate for any components that fail. This gives employees the window of opportunity to replace any failing components without the threat of a service

outage. However, if your system is running off of obsolete components, the application may not transition from one component to another, making the likelihood of service outage more likely.

If failure does occur, and the system is restored via back-up, will the system function correctly?

Make sure that you have back-up copies of all of your applications as well as copies of all your information. Many applications utilize system components or program modules that may be spread through an operating system. Back-up copies of the critical applications and any application updates, ensure that you can reinstall to a state prior to the failure.

Has your organization identified its most critical systems?

Identification of your organization's most critical I.T. systems should occur during the assessment stage of developing your disaster plan. You must identify the order of which systems in your organization should be

recovered first, based on their priority. While minutes of downtime may have serious consequences for some systems, other systems may go undone for weeks with no rising issues. The identification of critical systems should coincide with your business priorities.

Section II

RECOVERY AFTER THE DISASTER. Recovery following a disaster is a two-fold process that will involve both short term and long term recovery planning. And while you may feel the need to focus on your business and corresponding customers, the well-being of you, your family and your employees should come first. Having an effective method of communication between your companies and customers will allow your organization to progress forward in order to best serve your customers and yourself.

Remember, Safety First!

After the catastrophe has passed, remember that first and foremost, your primary concern is the safety of yourself and your family. You should first assess the status of your family and property before contacting your employer and/or employees.

Managers/supervisors should also check on the well-being of staff members following a disaster. An established telephone tree, noted in the development of a disaster plan, should be executed in order to determine the status of staff members.

Alternative housing or transportation needs may need to be arranged for staff members and be aware that not all staff members may be able to return immediately to work (due to injuries, home damage, family concerns, etc.).

Once all staff members and the state of their homes and family have been assessed, the well-being and status of the organization should now come into play. Never attempt to reenter your office or attempt repairs unless it is safe to do so. Be aware of broken or down power lines, protruding objects, broken glass, splintered wood and wet, slippery walkways. **DO NOT** use electrical appliances that have been exposed to water unless okayed by an electrician.

Consider a Back-Up Facility

If your primary office is inoperable, you will need a back-up facility. In the event your building becomes uninhabitable or inoperable due to a

major catastrophe, a pre-determined back-up facility can serve as a temporary office work site. Identify promising locations or sites and make contact with the owner or leasing agent so that any necessary arrangements to use their facility can be made on short notice following a disaster scenario.

Your back-up facility should be prepped in light of an oncoming disaster with enough supplies and materials for it to serve as a temporary and functional office. Your back-up facility should be stocked with a variety of items that will provide the resources you need in order for your operation to stay functional. A disaster supply kit should be readily available.

Communication Is the Key

After you have made assessments of your organization's staff members and the facilities, you will need to focus on the concerns of your clients. Any type of major disaster, whether a hurricane,

Keep in Touch

In order for the FLSO to properly serve both member agents and consumers, agency/agent emergency contact information should be reviewed annually.

This information provides FLSO with the most effective means to contact and assist you following a major disaster.

To update your contact information, please see the Catastrophe Contact Form found in the Informational Resources section on page 53.

tornado, flood or fire can be a nightmare for an insurance agency. Be prepared to be overwhelmed by customers and to work longer hours.

Staff members who are able to return to the office immediately following a storm should meet briefly to survey the damage and its impact on your customers. Teams and their responsibilities should be reiterated at this time.

If your area was hit by a major catastrophe, then you might be faced with an electricity loss. Major “life-lines” such as computers and telephones will not be operable without a second source of power. Generators may serve as a secondary power source – and should be purchased far in advance of a pre-determined disaster. If you use a generator to power computer equipment, you may also want to consider investing in an uninterrupted power supply (UPS) system to protect computer equipment from uneven current flow.

Loss of power and/or downed power lines will also affect how you may carry on telecommunications. Consider having non-electronic telephones available for use and wireless Internet cards for computers/laptops. Cellular phones will also provide a second method of communication between office staff and customers. If you utilize cellular phones to conduct business, make sure you have plenty of extra batteries and battery chargers.

A. Disaster Recovery Team Operations and Logs

The leader for each disaster recovery team should document their team’s activities by using a disaster recovery log (see Informational Resources section for a template example). This log should be used to prepare status reports for the Emergency Management team and should be used to

coordinate the concurrent activities of the other teams. All disaster teams should actively use the Disaster Recovery Log.

B. Customer Relations

Good communication with your customers will aid in the retention of an outstanding business relationship in the future. Utilize the convenience of voice mail, but only after closing down for the day. While a customer may get frustrated with a constant busy signal or being put on hold, they may become equally agitated if they leave a voicemail and their message is not returned.

Follow-up with your customers. Make sure you document the date you reported their claim’s information and include the name, address, and telephone number of the adjusting organization. A follow-up letter is an excellent method to document this information while giving your customers the piece of mind that they are being taken care of.

C. Company Relations

Again, communication is the key here. Make contact with your companies both before and after a catastrophe. Contacting them before a disaster will allow you the opportunity to make sure that all of your emergency contacts and procedures with them are current. Contacting them after a disaster is equally as important so you can be made aware of current decisions put into effect as a result of the disaster.

D. Employee Relations

Working in an insurance agency following a major catastrophe can be grueling. Staff members that are available to work, should expect long hours. Employees should be rotated out in order to give everyone breaks. Consider stocking food items on site as food supplies and transportation may be



scarce following a disaster. Employees should take full breaks when possible in an effort to minimize a highly stressful situation.

You must also take into account that if a hurricane or similiar disaster impacted your organization's area directly, you may lose a significant percentage of your staff. Make sure your organization has procedures in place for employee leave following a disaster.

Encourage your employees to also develop a family disaster plan complete with evacuation procedures, emergency contact numbers, list of important documents that must be take care of, and all disaster supplies. You may want to incorporate their disaster plans into your organization's.

INFORMATIONAL RESOURCES. This section contains a variety of charts and forms that may prove useful as you begin developing your own disaster plan. These items may be used as templates as you begin to customize your organization's disaster plan.

The World Wide Web may serve as your greatest resource for locating multiple resources of information. The following websites were used during the creation of this manual and may prove helpful while building your disaster plan:

American Red Cross
www.redcross.org

**Federal Emergency
Management Agency**
www.fema.gov

**Florida Department of
Financial Services**
www.fdfs.com

**National Hurricane
Center**
www.nhc.noaa.gov

- 1) Ready.gov Sample Business Continuity & Disaster Preparedness Plan
- 2) Employee Contact List Form
- 3) Building Your Disaster Plan: A Checklist for Existing Controls
- 4) Saffir-Simpson Hurricane Scale
- 5) Statewide Evacuation Routes (Map)
- 6) Back-Up Facility Supply Kit
- 7) Important Telephone Numbers
- 8) Disaster Recovery Log Template
- 9) FLSO Catastrophe Information Form

Business Continuity and Disaster Preparedness Plan

PLAN TO STAY IN BUSINESS

Business Name

Address

City, State, Zip Code

Telephone Number

The following person is our primary crisis manager and will serve as the company spokesperson in an emergency.

Primary Emergency Contact

Telephone Number

Alternative Number

E-mail

If this location is not accessible we will operate from location below:

Business Name

Address

City, State, Zip Code

Telephone Number

If the person is unable to manage the crisis, the person below will succeed in management:

Secondary Emergency Contact

Telephone Number

Alternative Number

E-mail

EMERGENCY CONTACT INFORMATION

Dial 9-1-1 in an Emergency

Non-Emergency Police/Fire

Insurance Provider

Business Continuity and Disaster Preparedness Plan (cont'd)

PLAN TO STAY IN BUSINESS

The following natural and man-made disasters could impact our business:

- _____
- _____
- _____
- _____

EMERGENCY PLANNING TEAM

The following people will participate in emergency planning and crisis management.

- _____
- _____
- _____
- _____
- _____

WE PLAN TO COORDINATE WITH OTHERS

The following people from neighboring businesses and our building management will participate on our emergency planning team.

- _____
- _____
- _____
- _____
- _____

OUR 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
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Business Continuity and Disaster Preparedness Plan (cont'd)

SUPPLIERS AND CONTRACTORS

Company Name: _____
Street Address: _____
City: _____ State: _____ Zip Code: _____
Phone: _____ Fax: _____ E-mail: _____
Contact Name: _____ Account Number: _____
Materials / Service Provided: _____

If this company experiences a disaster, we will obtain supplies/materials from the following:

Company Name: _____
Street Address: _____
City: _____ State: _____ Zip Code: _____
Phone: _____ Fax: _____ E-mail: _____
Contact Name: _____ Account Number: _____
Materials / Service Provided: _____

If this company experiences a disaster, we will obtain supplies/materials from the following:

Company Name: _____
Street Address: _____
City: _____ State: _____ Zip Code: _____
Phone: _____ Fax: _____ E-mail: _____
Contact Name: _____ Account Number: _____
Materials / Service Provided: _____

Business Continuity and Disaster Preparedness Plan (cont'd)

EVACUATION PLAN FOR _____ **LOCATION**
(Insert Address)

The following natural and man-made disasters could impact our business:

- 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 ____ times a year.

If we must leave the workplace quickly:

1. Warning System: _____

We will test the warning system and record results ____ times a year.

2. Assembly Site: _____

3. Assembly Site Manager & Alternate: _____

a. Responsibilities Include:

4. Shut Down Manager & Alternate: _____

a. Responsibilities Include:

5. _____ is responsible for issuing all clear.

Business Continuity and Disaster Preparedness Plan (cont'd)

SHELTER IN PLACE PLAN FOR _____ LOCATION
(Insert Address)

The following natural and man-made disasters could impact our business:

- 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 ____ times a year.

If we must take shelter quickly:

1. Warning System: _____

We will test the warning system and record results ____ times a year.

2. Storm Shelter Location: _____

3. "Seal the Room" Shelter Location: _____

4. Shelter Location & Alternate : _____

a. Responsibilities Include:

5. Shut Down Manager & Alternate: _____

a. Responsibilities Include:

6. _____ is responsible for issuing all clear.

Business Continuity and Disaster Preparedness Plan (cont'd)

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 location:

RECORDS BACK-UP

_____ is responsible for backing up our critical records including payroll and accounting systems.

Back-up records including a copy of this plan, site maps, insurance policies, bank account records and computer back ups are stored onsite _____.

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:

Business Continuity and Disaster Preparedness Plan (cont'd)

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 _____.

EMPLOYEE CONTACT INFORMATION LIST

It is imperative for the continuity of any viable business to maintain communications with its employees. Collecting basic contact information from each employee is necessary in order for an employer to make contact with the employees of the organization. In the event of an evacuation, employees may disperse to shelters or the homes of friends or relatives - make sure you have a method to contact employees through a third party should direct contact fail.

Name: _____

Position: _____

Key Responsibilities: _____

Home Address: _____

City, State, Zip: _____

Home Phone: _____ Cell Phone: _____

Office Phone: _____ Pager/Beeper: _____

Fax: _____

Home Email: _____ Work Email: _____

Emergency Contact: _____ Relationship: _____

Emergency Contact Phone: _____ Alt. Phone: _____

Notes: _____

Building Your Disaster Plan: A Checklist for Existing Controls

The checklist has been broken down into major categories: General Overview, Data Center Facility, Data Entry, Data Control, Computer Room, Tape Library, Telecommunications, Systems and Programming, Technical Support, Database Administration, Internal Audit, Insurance, Backup Facility, and Reciprocal Agreements. Many of the categories relate directly to sections in the Disaster Recovery Plan. After each question is space to answer “YES,” “NO” or “Work in Progress (WIP).” There is also a place to enter a notation as to who is assigned to complete the item or what action is planned. The checklist is designed to be a working paper that can be updated as events occur.

GENERAL OVERVIEW

	Yes	No	WIP	Assign/Action
1. If a major disaster to your data center occurred today, could your organization survive?				
2. Have you recently completed an Impact/Risk Analysis?				
3. Do you know the total dollar amount of your exposure?				
4. Have you prioritized all of your programs?				
5. Have you listed the maximum downtime for all of your systems?				
6. Have you listed the objectives of a disaster plan and the assumptions it includes?				
7. Do you have a disaster plan, and is it current?				
8. Does the Plan include backup facilities? Hot backup site? Cold site? Reciprocal agreement?				
9. Does the backup facility inform you when there is a change in hardware or software?				
10. Have you determined the cost of a disaster plan including: Initial cost? Development cost? Maintenance cost?				

11. Has top management approved the plan?				
12. Do you have a Disaster Planning Coordinator?				
13. Is someone assigned to update the plan?				
14. Does the plan use a team approach?				
15. Do you have people assigned to lead each team?				
16. Is the same person assigned to lead more than one team?				
17. Are names and phone numbers updated regularly?				
18. Have the Internal Audit, Security, and Insurance Departments reviewed the plan?				
19. Does the plan provide for recovery from a major disaster, and can it be adjusted for a less severe occurrence?				
20. Has the plan been tested using only material stored off-site?				
21. Is the plan tested at least every 6 months?				
22. Has the plan been updated as a result of the testing?				
23. Have you ever initiated a surprise test?				
24. Does the plan provide instructions for: Emergency procedures? Organizational structure following a disaster? Off-site storage for all recovery material?				
25. Does the off-site storage have 24-hour access, physical security, vaulting, fire protection, courier service, round trip travel time of less than 1 hour, access only by authorized persons?				

26. Are the tapes secured in a separately controlled room within the secured area?				
27. Is all system documentation, except program listings, kept in fireproof storage when not in use?				
28. Are there written instructions that define the responsibilities that personal computer (PC) users have for backing up and protecting their files?				
29. Have these instructions been given to all PC users?				
30. Have all data center personnel been advised about the confidentiality of all information they work with?				

DATA CENTER FACILITY

	Yes	No	WIP	Assign/Action
1. Are there signs outside identifying the data center				
2. Do security guards, fences, alarm systems, and/or closed circuit monitoring protect the building?				
3. Is wiring for all security and alarm systems passed through conduit?				
4. Do the guards make scheduled rounds of the building?				
5. If no guards are used, are the people responsible for security trained by security professionals?				
6. Has someone been assigned the responsibility for security of the data center, company, or building?				
7. Are security personnel or computer room personnel on-site at all times?				
8. Is there card access to the facility and various areas in the facility?				

9. Do all employees wear identification badges?				
10. Are visitors required to sign in and sign out?				
11. Is their security at the receiving area?				
12. Is there an Office/Building Emergency Booklet published that includes: Medical emergencies? Fire emergency procedures? Evacuation procedures? Bomb threats? Security violations? Electrical failures?				
13. Has someone been assigned to provide information, instruction, and supervision for the list in Item 12?				
14. Are evacuation route drawings posted in all hallways?				
15. Have all occupants been instructed and trained in emergency procedures?				
16. Are fire drills conducted on a regular basis under the supervision of your local fire marshal?				
17. Is there a written termination procedure that includes a checklist of items to be returned to the company, such as keys, ID badges, card access, etc.?				
18. Are all employees required to take vacation time so others can perform their duties?				
19. Do all areas of all buildings have a fire alarm system?				
20. Has the fire detection and extinguishing equipment been tested and/or inspected in the past 6 months?				

21. Does the insurance company or fire department make annual fire inspections?				
22. Is the storage area for forms and supplies protected with sprinklers?				
23. Are smoke detectors located in the storage area?				

DATA ENTRY

WIP

	Yes	No		Assign/Action
1. Are there alternatives for entering input normally keyed on-line?				
2. Have you made provisions to have keying done on the outside in emergencies?				
3. Is a copy of the keying instructions stored off-site?				
4. Is a software package used for keying, and is it available to outside services?				
5. Have arrangements been made to have your affiliates or divisions key your input?				
6. Are all manual procedures performed by data entry documented and a copy stored off site?				
7. Are source documents batched and controlled by another department?				
8. Are source documents stamped with date, time, and operator after keying?				
9. Are source documents maintained in their original batches for a short time so they can be re-keyed if necessary?				
10. Are source documents returned to the data control department after keying?				

11. Can the data entry department be reestablished in another location in a reasonably short time if necessary?				
---	--	--	--	--

DATA CONTROL

	Yes	No	WIP	Assign/Action
1. Is access to the data control department restricted?				
2. Are all source documents and computer reports routed through this department for control and balancing?				
3. If communication fails for transmitted reports, has an alternate method for sending reports to users been established?				
4. Is this department responsible for the control of check forms?				
5. Is there a written procedure for issuing a supply of blank checks outside the computer room?				
6. Are checks signed by a different person from the person balancing and distributing them?				
7. Can the check signer be replaced overnight?				
8. Is there any special office equipment critical to the operation of the data center, which provisions for a substitute have not been made?				
9. Are backup signature facsimiles secured off-site?				
10. Is there a formal custom-form system that identifies all forms, their reorder point, their supplier, and an alternate supplier?				
11. Is a small supply of all critical custom forms maintained on-site?				

12. Is a copy of all form specifications and a copy of the final proof maintained off site?				
13. Is a fact sheet maintained on all suppliers of office equipment and forms?				
14. Has an alternate point-to-point pickup and delivery been planned for if the primary method is not operational?				
15. Is there an output distribution reporting form for every printed report defining: number of copies, decollate, burst method of shipping, recipient name, and recipient phone number?				

COMPUTER ROOM

	Yes	No	WIP	Assign/Action
1. Is access to the computer room restricted?				
2. Are only the computer operators allowed to operate the computer?				
3. Do Halon, CO, or sprinklers protect the room?				
4. Are smoke detectors located: In the ceiling? Under the raised floor? In the air conditioning ducts?				
5. Will the smoke detectors operate even if there is a power outage?				
6. Are fire extinguishers located at all exit doors?				
7. Are water detectors located under the floor?				
8. Are waterproof covers stored in the computer room for emergencies?				

9. Is a UPS system installed for short power outages?				
10. Is a generator available for extended power outages?				
11. Is there emergency lighting in the computer room?				
12. Is there an emergency Power-Off switch located at the exits?				
13. Is there more than one cooling system that will support the computer hardware should one system fail?				
14. Will an alarm sound if the air conditioning system is turned off?				
15. Is the temperature and humidity monitored?				
16. Will some type of visible or audible alarm sound if the limits are exceeded?				
17. Are fire doors installed at all entrances to the computer room?				
18. Are check forms stored in a secured room?				
19. Are there written instructions for powering up and powering down the system?				
20. Are there written instructions for actions to take in an emergency?				
21. Is there a copy of the Disaster Recovery Plan in the computer room?				
22. Is a procedure library used that contains all the job control necessary to execute job streams?				

23. Is there a formal scheduling system, either computerized or manual?				
24. Is someone assigned to review the schedule and enter all control record information?				
25. Is the entering of control records and similar job control functions eliminated from operator intervention?				
26. Are tape mounts controlled by a tape-librarian system?				
27. Does a supervisor review reasons why an operator overrides the tape-librarian system?				
28. Does operations management review the console log and error listing to ensure that identifiable errors are corrected and recurring errors are prevented?				
29. Are there written restart procedures for all production systems?				
30. Do the restart procedures indicate that other systems may have to be reprocessed even though they completed successfully?				
31. Do all high priority systems have detail recovery procedures documented?				
32. Are all problems in the computer room documented?				
33. Are metered hours correlated to lapsed time if practical?				
34. Is there a formal Problem Management system, where computer room problems are reviewed by members from operations and programming and remedies assigned?				
35. Does operations management review all down time?				

36. Is all production job control reviewed by the operations department after testing is completed and before programs are turned over for production?				
37. Are there Run Manuals for all production applications?				
38. Do the operators have easy access to the Run Manuals?				
39. Are duplicate copies of the Run Manuals stored off site?				
40. Is all special processing for quarterly or annual runs properly documented?				
41. Are batch jobs scheduled for each shift?				
42. Is there a computerized job-accounting system?				
43. Is the job-accounting report reviewed to determine any unusual run patterns?				
44. Are all new systems reviewed for proper file rotation to off-site storage?				
45. Is there a list of all computer hardware including serial numbers, communication equipment and lines, power requirements, cooling requirements, floor space requirements, and acceptable substitute equipment for all the above; and is a copy of this list stored off-site?				
46. Is there a cable layout diagram and plug connector description for the current equipment, and is a copy stored off site?				
47. Is a Vendor Information sheet maintained for all vendors supplying computer equipment and supplies?				

48. Have you asked a used hardware vendor for a list of available equipment, in preparation for an emergency?				
49. Are the following backed up daily and rotated off site: Procedure library? Tape librarian? Job scheduling?				
50. Is there a formal procedure for making a program obsolete?				
51. Are the microfiche procedures documented and a copy stored off-site?				
52. Are there any water pipes near or above the computer room?				
53. Is there a threat of water leakage from nearby areas: kitchen, rest rooms, janitor closet, and drinking fountain?				

TAPE LIBRARY

	Yes	No	WIP	Assign/Action
1. Do Halon, CO, or sprinklers protect the tape library?				
2. Are smoke detectors located in the tape library?				
3. Does the entrance to the tape library have a fire door?				
4. Does the tape library have emergency lights?				
5. Does card access or other security restrict access to the tape library?				
6. Is a fire extinguisher mounted outside the door to the tape library?				

7. Has the tape library become a storage area for items other than tapes?				
8. Does the off-site storage for tapes have security, fire protection, 24-hour access, bonded pickup and delivery?				

SYSTEMS AND PROGRAMMING

	Yes	No	WIP	Assign/Action
1. Is all application software backed up and stored off site?				
2. Do all changes to programs need authorization?				
3. Are there audit trails that identify any program that has been copied for modification, or new program in development?				
4. Is all application software responsible for distributing funds, such as payroll and accounts payable, password protected?				
5. Do the systems above have adequate controls, such as batch totals, hash totals, run totals, and dollar amounts?				
6. Are checks outside the normal range flagged on an audit trail report?				
7. Does an accounts payable audit trail report list the payee for all checks?				
8. Do all financial applications have complete audit trail reports?				
9. Is all of the on-site system documentation stored in fireproof cabinets?				
10. Are users asked to assist in the preparation of test data?				

11. Is there a formal methodology for design and programming?				
12. Is the design phase completed before the programming phase begins?				
13. Are there written design standards and programming standards?				
14. Are 311 permanent files categorized as critical, important, useful, and non- essential?				
15. Do the standards require the backing up of all critical files?				
16. Are the 3 most current generations of all-important and critical files maintained (current, father, grandfather)?				
17. Do the standards require all programs to include proper controls and totals for complete auditing, and for the detection and correction of errors?				
18. Is test data with predetermined results saved and used for heavily maintained systems such as payroll?				
19. Are program changes always made to the source code?				
20. Is the source code maintained in a library that is backed up and rotated off-site?				
21. Are the program link-edit reports reviewed for errors and filed with the source code listing?				
22. Are programs always tested even when they have minor modifications?				
23. Does management randomly review program changes and test results?				

24. Do user department's sign off on program modifications and review test results?				
25. Is there a formal procedure for making a program in development a production program?				
26. Are operation Run Manuals required as part of the program turnover to operations?				
27. Are all modifications to purchased software fully documented and coded in a way that will not disturb the pure supplied code?				
28. Is a list available of all systems with the person responsible noted?				
29. Is there a list that identifies all programs in a system?				
30. Does each system have a back-up person?				
31. Is documentation kept current?				
32. Is documentation maintained on the computer, backed up, and rotated off-site?				
33. Is there a listing of all technical manuals so they can be replaced if necessary?				
34. Does your company policy state the retention period for corporation assets information, stockholder information, tax records, employee information, and other vital records?				
35. Are record layouts maintained for the retention period along with the file media?				
36. Has the source information been identified that created the retained data?				

TECHNICAL SUPPORT

	Yes	No	WIP	Assign/Action
1. Is the operating system backed up and rotated off-site?				
2. Is a list maintained of all operating system software?				
3. Are the people in the department cross-trained so that everyone has backup?				
4. Are all responsibilities, duties, and procedures documented and a copy stored off site?				
5. Is a Vendor Information sheet maintained for all vendors supplying software?				
6. Have provisions been made for purchased software to execute on another system during an emergency?				
7. Is a copy of the SYSGEN parameters stored off-site?				
8. Is there complete documentation explaining how to bring up the operating system at the backup facility?				
9. Is the utilization of all disk devices documented?				
10. Has a plan been formulated on how alternate disk devices would be utilized?				
11. Is there documentation explaining how to modify the JCL to execute at the backup facility?				

DATABASE ADMINISTRATION

	Yes	No	WIP	Assign/Action
1. Are all databases identified?				
2. Are all programs that update each database identified?				

3. Is the activity that updates the database continually logged?				
4. Are all programs that access each database identified?				
5. Are databases backed up and rotated off-site?				
6. Are audit trails available that identify databases that are filing up, and are these reports available on a daily basis?				
7. Are there documented procedures on how to test the validity of each database after it is restored?				
8. Is there documentation that identifies multiple databases that must be kept synchronized with each other?				

INTERNAL AUDIT

	Yes	No	WIP	Assign/Action
1. Have you reviewed the, Disaster Recovery Plan?				
2. Have you observed a recovery test that only used material stored off-site?				
3. Do you periodically review the data center operation and make written recommendations on improvements to procedures, security, and controls?				
4. Are user departments required to balance computer output to manual control totals for audit and security?				
5. Do you save test data to process through cash disbursement systems producing predetermined results?				

INSURANCE

	Yes	No	WIP	Assign/Action
1. Has the data center management been informed as to the dos and don'ts concerning insurance following a disastrous event?				
2. Does the insurance policy include business interruption coverage?				
3. Is another department in the organization responsible for insurance protection?				
4. Do you have a copy of the insurance policy?				
5. Have you reviewed the coverage in the past year?				
6. Do you have an annual formal review of your insurance coverage with the insurance carrier?				
7. Does the insurance coverage include data processing hardware and software?				
8. Did you perform a risk/impact analysis for the data center?				

BACKUP FACILITY

	Yes	No	WIP	Assign/Action
1. Do you currently subscribe to a fully equipped backup facility?				
2. Is the backup facility located at a distance that will ensure that an area-wide disaster will not affect the facility?				
3. Is the security at the backup facility at least as good as the security at your current facility?				
4. Have you ever used the backup facility as part of a mock disaster?				

5. Does the backup facility have adequate hours available for testing?				
--	--	--	--	--

RECIPROCAL AGREEMENTS

	Yes	No	WIP	Assign/Action
1. Do you have a formal reciprocal agreement currently in effect?				
2. Does the other organization's computer have time available to share with you?				
3. Does your computer have time available to share with another organization?				
4. Are both computer systems compatible?				
5. Do both computer systems have the capacity to process critical applications for both organizations at the same time?				
6. Is the operating system software compatible?				
7. Is there sufficient tape and disk capacity and compatibility?				
8. Will your communication network quickly connect with the other organization's computer?				
9. Does either data center have specialized hardware such as laser printers or cartridge tape drives?				
10. Have both organizations agreed to notify the other about changes in hardware or software?				
11. Will your purchased software execute at the other data center?				

12. Have you tested a critical application at the other data center?				
13. Is there temporary storage available at the other data center for printer forms?				
14. Is there temporary storage available at the other data center for your tape library?				
15. Is there temporary office space available at the other data center for operations support personnel?				



Saffir-Simpson Hurricane Scale

Category	Definition	Effects
One	Winds 74-95 mph	No real damage to building structures. Damage primarily to unanchored mobile homes, shrubbery, and trees. Also, some coastal road flooding and minor pier damage
Two	Winds 96-110 mph	Some roofing material, door, and window damage to buildings. Considerable damage to vegetation, mobile homes, and piers. Coastal and low-lying escape routes flood 2-4 hours before arrival of center. Small craft in unprotected anchorages break moorings.
Three	Winds 111-130 mph	Some structural damage to small residences and utility buildings with a minor amount of curtainwall failures. Mobile homes are destroyed. Flooding near the coast destroys smaller structures with larger structures damaged by floating debris. Terrain continuously lower than 5 feet ASL may be flooded inland 8 miles or more.
Four	Winds 131-155 mph	More extensive curtainwall failures with some complete roof structure failure on small residences. Major erosion of beach. Major damage to lower floors of structures near the shore. Terrain continuously lower than 10 feet ASL may be flooded requiring massive evacuation of residential areas inland as far as 6 miles.
Five	Winds greater than 155 mph	Complete roof failure on many residences and industrial buildings. Some complete building failures with small utility buildings blown over or away. Major damage to lower floors of all structures located less than 15 feet ASL and within 500 yards of the shoreline. Massive evacuation of residential areas on low ground within 5 to 10 miles of the shoreline may be required.

Hurricane Watches and Warnings

A hurricane watch is issued when there is a threat of hurricane conditions within 24-36 hours. A hurricane warning is issued when hurricane conditions (winds of 74 miles per hour or greater, or dangerously high water and rough seas) are expected in 24 hours or less.

Back-Up Facility Supply Kit

Emergency Supplies	Office Supplies	Personal Supplies
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> First Aid Kit / Medicines / Prescription Drugs <input checked="" type="checkbox"/> Flashlight / Lanterns <input checked="" type="checkbox"/> Batteries <input checked="" type="checkbox"/> Radio – battery operated and NOAA weather radio <input checked="" type="checkbox"/> Heavy-duty tape <input checked="" type="checkbox"/> Regional maps <input checked="" type="checkbox"/> Candles <input checked="" type="checkbox"/> Matches / Butane lighters <input checked="" type="checkbox"/> Scissors <input checked="" type="checkbox"/> Dust or filter masks <input checked="" type="checkbox"/> Hand tools (wrench, pliers, etc.) <input checked="" type="checkbox"/> Generator* <p>*NOTE: When considering a generator, take the following factors into consideration before purchase:</p> <ol style="list-style-type: none"> 1. What size generator will you need (kilowatt/KW power)? 2. What type of generator will best serve your situation (plug-in vs. hardwired)? 3. What type of fuel should be used (gas, diesel, natural gas)? 4. What is the rate of fuel usage? 5. What type of fuel storage will be necessary and what is available? 6. What type of maintenance supplies will be needed for extended use? 7. What kind of security will be available for your generator at night? 	<p>General Office Supplies:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> File Folders <input checked="" type="checkbox"/> Pens <input checked="" type="checkbox"/> Stamps <input checked="" type="checkbox"/> Envelopes <input checked="" type="checkbox"/> Stapler and staples <input checked="" type="checkbox"/> Paper clips <input checked="" type="checkbox"/> Carbon Paper <input checked="" type="checkbox"/> Printer paper <input checked="" type="checkbox"/> Notepads <input checked="" type="checkbox"/> Post-it Notes <input checked="" type="checkbox"/> Business/Contact cards <input checked="" type="checkbox"/> Claim Forms <input checked="" type="checkbox"/> Maps (these will come in handy when you have incoming adjusters that are unfamiliar with the area) <p>Computer Equipment:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Laptop Computer <input checked="" type="checkbox"/> Wireless Internet Card <input checked="" type="checkbox"/> Small, portable printer 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Water – at least 1 gallon daily per person for 3-7 days <input checked="" type="checkbox"/> Food – at least enough for 3-7 days: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> non-perishable packaged or canned food/juices <input checked="" type="checkbox"/> snack foods <input checked="" type="checkbox"/> non-electric can opener <input checked="" type="checkbox"/> cooking tools/fuel <input checked="" type="checkbox"/> paper plates/plastic utensils <input checked="" type="checkbox"/> paper towels <input checked="" type="checkbox"/> cups <input checked="" type="checkbox"/> coffee / sweetener / creamer / instant coffee and/or tea <input checked="" type="checkbox"/> soft drinks <input checked="" type="checkbox"/> Aspirin / Tylenol, etc. <input checked="" type="checkbox"/> Trash cans and bags <input checked="" type="checkbox"/> Clothing – seasonal / rain gear / sturdy shoes <input checked="" type="checkbox"/> Blankets / Pillows, etc. <input checked="" type="checkbox"/> Toiletries / Hygiene Items / Moisture Wipes <input checked="" type="checkbox"/> Petty Cash – Banks and ATMs may not be open or available for extended periods <input checked="" type="checkbox"/> Keys <input checked="" type="checkbox"/> Books and Games <input checked="" type="checkbox"/> Important documents – in a waterproof container <input checked="" type="checkbox"/> Insurance, medical records, bank account numbers, Social Security cards, etc. <input checked="" type="checkbox"/> Vehicle fuel tanks filled

Important Telephone Numbers

American Red Cross Donations	800.RED.CROSS
Attorney General's Price Gouging Hotline	866.966.7226
Contractor License Verification	866.532.1443
Department of Education School Information	888.665.5055
Department of Financial Services Insurance Claim Hotline	877.MY.FL.CFO
Elder Services Hotline	800.96.ELDER
FEMA	800.621.FEMA
Florida Division of Emergency Management	850.413.9969
Florida Power and Light Hotline	800.4.OUTAGE
Florida Records Storage Center	850.245.6750
Florida State Courts Information	850.922.5081
Progress Energy Hotline	800.228.8485
Road Information	511
Salvation Army Donation Helpline	800.SAL.ARMY
State Volunteer and Donations Hotline	800.FL.HELP1

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

FSLSO Catastrophe Information Form

In case of a catastrophic situation Florida's insureds may be unable to contact your office. The FSLSO would like to help in such a situation by providing contact information to these insureds. To aid in this effort, please complete the information below and return to the FSLSO via fax or mail. (Email address: cdaniels@fslso.com Fax: (850) 513-9624)

Surplus Lines Agent Name: _____ License #: _____

Agency Name: _____

Agency Toll Free Number: _____

Telephone Number: _____ FAX Number: _____

Email Address: _____

Does your office have a Catastrophe Plan? _____ Yes _____ No

If yes, please provide the following information:

Claims Manager's Name: _____

Telephone Number: _____ FAX Number: _____

Email Address: _____

If no, how do you handle claims? _____

In case of a catastrophe and your office is not operational, how can we contact you, or who do we contact?

Please provide a list of eligible surplus lines insurers you place business with along with the insurer's catastrophe contact information.

