COOP for CBOs

Continuity of Operations
for Community-based Organizations

Volunteer Florida
The Elliot Building
401 S. Monroe Street
Tallahassee, FL 32301

www.volunteerflorida.org

Acknowledgements

This curriculum was assembled and organized by Volunteer Florida. Volunteer Florida gratefully acknowledges the contributions of the following organizations:

- Federal Emergency Management Agency
- Florida Department of Community Affairs, Division of Emergency Management
- Institute for Business & Home Safety
- Ocala-Marion County Economic Development Corporation
- Tampa Bay Regional Planning Council
- University of Wisconsin-Green Bay Center for Organizational Studies

A detailed list of the resources used in this curriculum appears in Unit 9.

Volunteer Florida
401 So. Monroe Street, Tallahassee, FL 32301
www.volunteerflorida.org

TABLE OF CONTENTS

CONTINUITY OF OPERATIONS for CBOs
COURSE OUTLINE

Unit One - Course Overview

A. Introduction
B. Administrative Announcements
C. Course Purpose
D. Course Goals
E. Instructional Material
    1. Text
    2. PowerPoint
    3. Students
F. Agenda
G. Student Introductions

Unit Two - Introduction to Continuity of Operations

A. Community-based Organizations
B. Survival
    1. Need
    2. Definition of COOP
    3. Significance
    4. Federal, state and local government initiatives
C. Continuity of Operations
    1. Process
    2. Elements
D. Governmental Continuity of Operations Initiatives
    1. Federal
    2. State and Local
E. Caveats
    1. Direct and indirect consequences
    2. Community versus individual disaster
    3. Upstream and downstream failures
    4. Research findings
        - Attitude
    5. Scale
        - Recognize huge variation in scale of CBOs and resources, and the consequent variety in plan complexity
E. Summary
    1. Who or what are you?
    2. What constitutes a disaster or emergency to you?
    3. What are your risks and vulnerabilities?
    4. What can you do to survive them?
    5. Flexibility, redefinition and attitude

Unit Three - Emergency Management

A. What is an Emergency?
B. What is Emergency Management?
C. Four Phases of Emergency Management
    1. Preparedness
    2. Response
    3. Recovery
    4. Mitigation

Unit Four - Potential Hazards

A. Natural
    1. Severe Weather Systems
    2. Flooding
    3. Extreme Heat and Drought
    4. Wildfire
    5. Sinkholes and Seismic Events
    6. Agricultural Diseases and Pests
    7. Human Disease Epidemics
B. Man Made
    1. Fire
    2. Hazardous Materials
C. Technological
    1. Technological Emergencies
    2. Power Service Disruption
    3. Environmental Health
    4. Radiological Emergencies
D. Criminal/Terrorism
    1. Terrorism
    2. Bomb Threats
    3. Building Explosion
    4. Suspicious Letters & Parcels
    5. Chemical & Biological Weapons
    6. Cyber Attacks
    7. Civil Unrest
    8. Robbery & Theft
E. Other Hazards
    1. Violence in the Workplace
    2. Internal Sabotage/Fraud/Theft
    3. Loss of Key Staff
    4. Workforce Disruption
F. Unique/Specific Hazards

What hazards do you face that are unique or specific to your own organization?

Unit Five - Preparedness

A. Purpose of Organization
    1. Reason for Existence
    2. Mission Essential Functions
B. Current Situation
C. Post-Disaster/Emergency Goal
D. Plan
    1. Process
        a. Establish a team
            - Revisit A, B & C
        b. The Planning Process
        c. The Continuity of Operations Plan
    2. Essential Elements
        a. Mission Essential Functions
        b. Current Resources and Capabilities
        c. Hazard Identification, Risk Assessment and Vulnerability
        d. Direction & Control
        e. Authority and Succession
        f. Logistics and Administration
        g. Security
        h. Communication
        i. Facilities & Equipment
        j. Vital Records and Databases
        k. People
        l. Supplies, Products & Services
        m. Insurance
        n. Community Relations
E. Exercise and Training
    1. Train, Test, Exercise & Modify
    2. Integrate the Plan into Organization Operations
    3. Establish Policy Guidance and Standards
    4. Training
    5. Testing
    6. Exercise
    7. Evaluation and Modification

Unit Six - Mitigation

A. Definition and discussion
    1. Mitigation = Prevention
    2. Soft Mitigation Measures
        a. Plan
        b. Organization
        c. Rules and Regulations
        d. Insurance

3. Hard Mitigation Measures
    a. Facilities & Equipment
    b. Response and Recovery Equipment & Supplies
    c. Disaster Supply Kit
    d. Disaster Go Kit

B. Discussion of Possible Mitigation Measures
    1. Building Fire
    2. Wildfire
    3. Hurricanes and Other Wind Storms
    4. Flooding
    6. Power Service Disruption
    7. Hazardous Materials
    8. Cyber Security and Vital Records
    9. Facility Security

Unit Seven - Response

A. Response
B. Decision to Activate Response Plan
    1. Immediate Pre-Event Preparation
    2. Functional Activation of Plan Elements
C. Notification
    1. Emergency Warnings/Alarms
    2. Emergency Management Group
    3. Internal
    4. External
    5. Call-down lists
D. Emergency Protective Actions
    1. In-house Sheltering
    2. Evacuation
    3. Facility/Operations Shutdown
    4. Other
F. Immediate Post-Disaster
    1. Human Life and Health
    2. Damage Control
    3. Damage Assessment

Unit Eight - Recovery

A. Implement Your Recovery Plan
    1. Gather Team
    2. Set Up Base of Operations
    3. Planning Considerations
    4. Continuity of Management
B. Periods of Recovery
    1. Immediate Emergency Period

Unit One
COURSE OVERVIEW

INTRODUCTION

ADMINISTRATIVE ANNOUNCEMENTS

COURSE PURPOSE

Introduce community-based organizations to a process that will help them survive potential emergencies and continue or reinstitute operations with minimal delay or interruption.

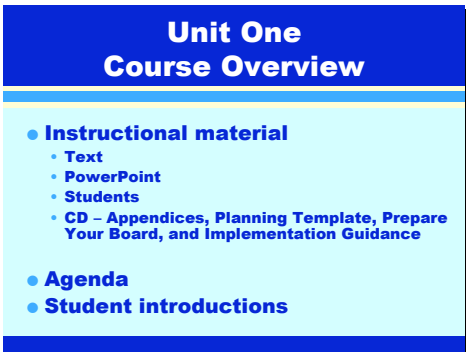
COURSE GOALS

At the conclusion of the training the student should:

- Understand the purpose and processes of emergency management
- Be familiar with the four phases of emergency management
- Be informed regarding governmental Continuity of Operations initiatives
- Have knowledge of hazards and potential emergencies
- Know the difference between hazards, risk and vulnerability
- Know the definition and components of Continuity of Operations planning
- Understand the Continuity of Operations planning process
- Know the essential elements of a Continuity of Operations plan
- Be familiar with training, testing and exercise concepts
- Be able to apply Continuity of Operations principles to his or her own unique organization

INSTRUCTIONAL MATERIAL

- Text
- PowerPoint
- Students
- CD – Template, Prepare Your Board, all Appendices and Implementation Guidance



AGENDA

STUDENT INTRODUCTIONS

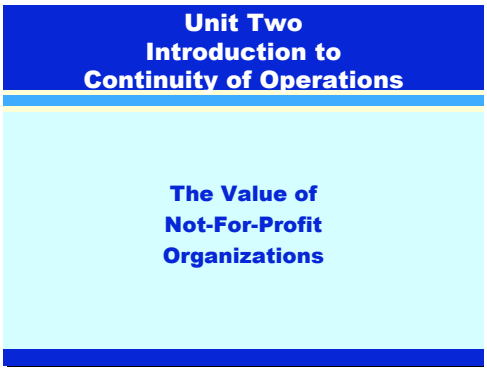
- Name
- Organization
- Position, length of time
- Emergency Management / Continuity of Operations experience
- Learning Goals

Unit Two
INTRODUCTION TO CONTINUITY OF OPERATIONS

COMMUNITY-BASED ORGANIZATIONS

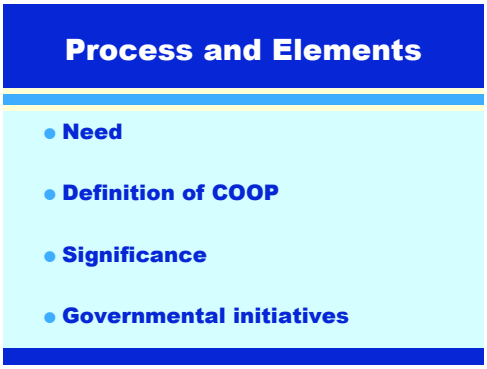
Community-based organizations constitute an extremely important component of the community. Not-for-profits contribute to the community economically and through the services they provide. More importantly, non-profits represent the time, energy and money the community has invested into making itself a better place to live.

Disasters further complicate the already complex relationships and dependencies between the community and not-for-profits. Recovery of not-for-profits is not solely an entrepreneurial or economic issue. Survival goals for not-for-profits and for the community are not independent of one another nor mutually exclusive.



CONTINUITY OF OPERATIONS

A Continuity of Operations plan is a process wherein your organization readies itself to deal with any emergency that affects its ability to continue normal operations. The plan prepares you to maintain and resume your operations after a disaster. It also presents you with the opportunity to examine how your organization currently operates and to improve current practices and procedures. The Continuity of Operations plan consists a process and certain essential elements, both of which will be thoroughly described in Unit 5. The Continuity of Operations plan will generally include plans, procedures, training and exercises as well as elements addressing:



- Safety of personnel and visitors
- Protection of facilities, equipment, supplies and products
- Protection of vital records and information
- Communications
- Management and authority
- Ability to continue essential operations
- Successful response and recovery

GOVERNMENTAL CONTINUITY OF OPERATIONS INITIATIVES

The Federal government has pursued a variety of operational continuity initiatives over the years (at both the agency and elected level) with the degree of effort fluctuating based on the magnitude of any perceived threats. In 1998, Executive Order 12656 required, "The head of each Federal department and agency shall insure the continuity of essential functions in any national security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records; and establishment of emergency operating capabilities."

The world became more threatening in the 1990's with the bombing of the World Trade Center, the bombing of the Federal building in Oklahoma City and the subway chemical attach in Japan. Subsequently, several Presidential Decision Directives (PDD's) were issued:

- PDD 39 — *US Policy on Counterterrorism*, 6/95
- PDD 62 — *Protection Against Unconventional Threats to the Homeland and Americans Overseas*, 5/98
- PDD 63 — *Critical Infrastructure Protection*, 5/98
- PDD 67 — *Enduring Constitutional Government and Continuity of Government Operations*, 10/98

In 1999, the newly designated Executive Agent, the Federal Emergency Management Agency, began developing a series of Federal Preparedness Circulars (FPC's) to provide specific implementation guidance on continuity of operations in accordance with Executive Order 12656.

- FPC 65 — *Federal Executive Branch Continuity of Operations*, 7/99
- FPC 66 — *Test, Training and Exercise (TT&E) Program for Continuity of Operations*, 4/01
- FPC 67 — *Acquisition of Alternate Facilities for Continuity of Operations*, 4/01

These Federal Preparedness Circulars, in concert with Executive Order 12656, constitute the framework of the Federal continuity of operations program.

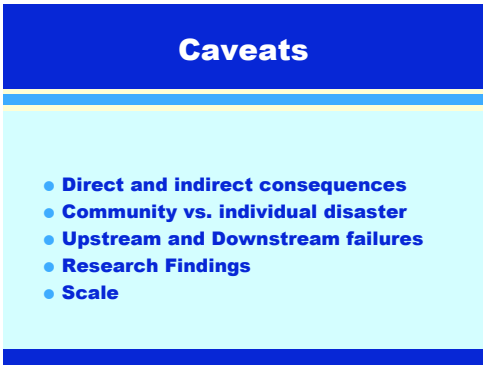
At the State of Florida level, emergency management in general and continuity of operations in particular are addressed in Chapter 252.365 of the Florida Statutes (F.S.), which is known as the Emergency Management Act. Governor's Executive Order (EO)

80-29 preceded the adoption of Ch. 252-365, F.S. and directed State agencies and counties to develop disaster preparedness capabilities. In 1987, the State Emergency Response Commission was established by EO 87-57, which also directed the formation of Local Emergency Planning Committees.

With recent events, the State has become even more proactive in emergency preparedness. Chapter 2002-43, Laws of Florida, amended Ch. 252.365, F.S., to require that each State agency create a disaster preparedness plan, specifically including a full-scale Continuity of Operation plan. The law also requires that each county government prepare for a possible disaster by developing a county-level Continuity of Operations plan. Many municipalities and other local government agencies are also involved in the process.

CAVEATS

The process of developing a Continuity of Operations plan can be extraordinarily complex. While this course does not go to the level of detail that would be covered in a more extensive training program, it will address all of the essential components of such a plan. The process of plan development is applicable to a federal or state agency, a large multi-national corporation or a small not-for-profit organization.



It is important to acknowledge, however, that the huge differences in the size of an organization and the resources available will have inherent ramifications in the complexity of any Continuity of Operations plan. What large operations need to do, and can do, may be impossible for a small organization to achieve. Smaller organizations should, therefore, become familiar with the entire process but be prepared to choose only those procedures that are most applicable to their own needs.

When considering the possible consequences of a disaster on your organization, do not be tempted to minimize risks with the thought that “it couldn’t happen to me.” It could happen to you. You could be directly impacted by any number of know or unknown hazards. Equally important is the fact that you could be indirectly impacted as a consequence of an emergency or disaster affecting someone else.

If the flow of goods and services to your organization is interrupted because of a supplier’s emergency, you will suffer adverse consequences. If your customers cannot accept your goods or services due to their own emergency, you are being affected by that emergency. In the event of a major disaster affecting your entire community, your organization may escape physical damage yet suffer devastating injury to its operation. When developing a Continuity of Operations plan, it is imperative to always keep the wider picture in mind.

In developing a Continuity of Operations plan it is important to recognize that the plan is for the continuance of your operation, not merely a plan for physical facilities. The physical component is an important part of the plan, for it supports the objective of continuity, but it is not the only, or even the most important consideration.

In fact, research has shown that attitude, adaptability and flexibility are fundamental requirements for organizational survival. One study[1] in particular listed five findings, each of which documented the weak linkage of business failure to physical damage and the strong linkages to more subjective factors. The authors concluded:

- Traditional structural precautions are necessary to reduce losses to life and property, but are not sufficient to insure organizational survival.
- Most organizations do not fail immediately after an event. Most organizations that ultimately fail do so only after a desperate struggle to recover.
- Most losses do not occur during or after an event. Agency losses go beyond initial damage to include business interruption, lost income to employers and employees and loss of organizational assets.
- Most owners have few ideas about how to recover. Many are so engaged in getting back to business as usual they fail to see the futility of their efforts. Survivors often come up with an alternate strategy, such as moving to a new location, changing their business processes or even changing their products or services. Survivors are flexible, innovative entrepreneurs.
- Multiple factors may be associated with a agency's success:
    - Organizations whose customers are unaffected by the disaster have a better chance than those whose customers have been impacted.
    - Organizations with more than one location have a higher survival rate
    - Organizations providing basic goods and services are less likely to fail than those depending on customer's discretionary income
    - Organizations who adjust to changes in customer demand survive better than those who doggedly pursue pre-disaster patterns.

SUMMARY

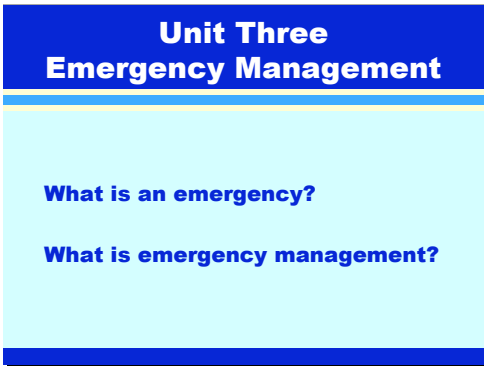
The Continuity of Operations plan is a tool that will help you persevere in the face of disaster. It is a process that should allow you to strengthen your organization. While the Continuity of Operations process is applicable to institutions of all types and sizes, it is incumbent upon you to use these guidelines to create the best possible plan for you own unique circumstances.

- What/who are you?
- What could constitute a disaster or emergency for your organization?
- What are your risks?
- What can I do to survive?
- Am I flexible enough to redefine my organization's purposes and processes?

[1] *Organizations At Risk: What Happens When Small Businesses and Not-For-Profits Encounter Natural Disasters*, University of Wisconsin-Green Bay Center for Organizational Studies, 2001

Unit Three
Emergency Management

WHAT IS AN EMERGENCY?



An emergency is any unplanned event that can cause deaths or significant injuries to employees, customers or the public; or that can shut down your Organization, disrupt operations, cause physical or environmental damage, or threaten the organization's public image or financial standing.

Obviously, numerous events can be emergencies, including

- Natural hazards like windstorms and floods
- Man-made emergencies such as a building fire
- Technological events like computer breakdowns
- Crime
- Terrorism
- Internal theft or sabotage
- Loss of key employees, suppliers or customers

An emergency is not necessarily a disaster. The term disaster implies a large-scale event. However, an emergency does not have to be large-scale to have serious consequences. Regardless of how it is categorized, each event must be evaluated in terms of the impact it has on your organization. What might constitute a nuisance to a large industrial facility could be a "disaster' to a Community Based Organization.

WHAT IS EMERGENCY MANAGEMENT?

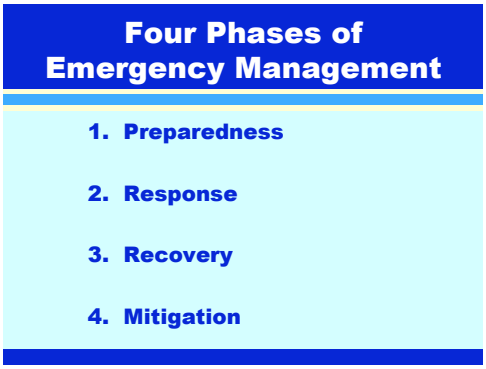
Emergency management is the process of preparing for, mitigating, responding to and recovering from an emergency. The process is cyclical in nature. A new emergency management program may be initiated in the preparedness stage, but once started each step follows naturally from the other in a regular and continuous manner.

It is also a dynamic process. Planning and reacting are critical activities, but not the only components. Training, conducting drills and exercises, testing equipment and coordinating the entire process internally and externally are other important factors.

An emergency management program, if supported by upper management and fully incorporated into the organization's culture, will:

- Protect lives and property
- Facilitate post-emergency recovery and Agency survival
- Reduce exposure to criminal or civil liabilities
- Possibly reduce insurance premiums
- Help fulfill the organization's responsibility to employees, suppliers, customers and the community
- Enhance the organization's image and credibility

FOUR PHASES OF EMERGENCY MANAGEMENT



Response
That part of the emergency management cycle that occurs immediately before, during, and immediately after an emergency event. It is not merely a reaction; it is a planned set of operations designed, to the extent possible, to manage and control the event and its consequences.

Recovery
Consists of restoring the physical and operational elements of an organization to their pre-disaster state. It may include modified, improved or alternative solutions.

Mitigation
Preventive measures taken to eliminate or reduce the risk of experiencing an emergency, and to reduce vulnerability and decrease potential damage and other adverse consequences.

Preparedness
The process of making an organization ready and able to implement the other three phases of emergency management.

Unit Four
POTENTIAL HAZARDS

This unit provides a brief overview of the many types of hazards that may threaten Florida's community-based organizations.

NATURAL HAZARDS

Severe Weather Systems

Severe weather systems are the most common major hazard in Florida. Included in this category are hurricanes, tropical storms, tornadoes, thunderstorms, winter storms, lightning and hail.

Hurricanes are tropical cyclones originating in the Atlantic Ocean or Gulf of Mexico during the warmer months (mostly from June to November). They are characterized by high winds, widespread torrential rains and flooding, and often by massive coastal storm surges. By definition, a hurricane has winds of 74 MPH and it can exceed 155 MPH. Winds above 111 MPH typically result in major damage. Flooding from hurricanes can extend far inland, result in extensive damage, and last for days, if not weeks, after the hurricane has passed. Storm surge consists of an abnormal rise in sea level that threatens life and property along the coastal areas.

Tornadoes are more localized than hurricanes, but can be in excess of a mile wide and can travel many miles before they dissipate. Unlike hurricanes, the warning time for tornadoes is extremely short and tornadoes frequently hit with no warning whatsoever. Most tornadoes have wind speeds of less than 110 MPH, but some tornadoes can approach 300 MPH. Florida is third in the nation in the annual number of tornadoes.

Even thunderstorms can produce extremely violent weather¸ producing straight line winds in excess of 100 MPH, causing dangerous flash flooding and producing hail and lightning.

While, hurricanes, tornadoes and thunderstorms are usually associated with warmer weather, Florida can also be the target of severe winter storms that wreak the same disastrous results as their summer cousins. Winter can also bring extreme cold that can be dangerous to people, animals and crops and immobilize areas that have limited experience in dealing with this type of weather.

Flooding

While flooding is a component of hurricanes and other severe weather, it merits independent consideration due to the magnitude of its impact on Florida and the rest of the country. Flooding can be deadly. More lives are lost due to flooding than any other danger associated with severe weather systems. As much as 90 percent of the damage related to all natural disasters (excluding drought) is causes by floods and associated debris flows.

Extreme Heat and Drought

Extreme heat is mostly a life safety issue, for people, animals and crops. These issues can also translates into workplace ramifications and have significant effect on businesses associated with tourism or agriculture. Not-for-profit agencies may affected due to the impact on their clients.

Drought results from abnormally periods of dry weather that can produce serious effects, particularly to agriculture. Major droughts can also create shortages in water supply, creating major consequences for urban as well as rural areas. The economic impact can be devastating. Drought also increases the risk of wildfires and flash floods.

Wildfire

While the possibility of a wildfire is greatly increased by extended droughts, the risk of such a fire always exists. The spring and fall seasons are dryer in general, and the winter is often referred to as the “fire season.” Fires can be started naturally, often from lightning, accidentally, or in many instances purposefully by arsonists. Wildfires have historically impacted forested or rural areas.

Sinkholes and Seismic Events

A limestone bedrock known as karst topography underlies much of Florida. Over time water is able to dissolve this bedrock, producing depressions, caverns, springs and sinkholes. Sinkholes occur when the roof of a natural underground cavern collapses. Sometimes this occurs gradually, but it is just as likely to be a sudden event resulting in property damage, injury or loss of life. As Florida has become more developed man’s

activities, such as pumping water, construction and changing drainage patterns, have increased the rate of sinkhole formation in the state.

Earthquakes are major hazards in many areas of the country, but are not considered to be a significant hazard in Florida.

Agricultural Diseases and Pests

Agricultural operations are extremely vigilant regarding diseases and pests that affect crops or animals. Not only are individual operations impacted, this hazard includes the risk of diseases and pests quickly spreading to others and infecting whole regions or perhaps the entire state. In addition to direct economic losses, agribusiness in general can be affected as well as the food and restaurant industry. The entire state economy, including those who have no direct ties to agriculture, can suffer severe consequences as a result of agricultural pests or diseases.

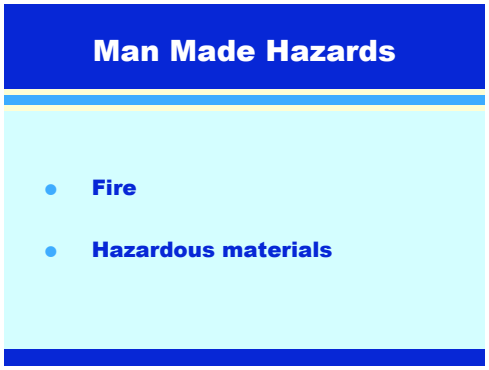
Human Disease Epidemic

Human diseases can have a wide-ranging effect and may be considered to be the most serious hazard face by mankind. Absenteeism due to a cold "going around town" can have slight to moderate impact on operations. More serious diseases can begin to affect suppliers and customers as well. While modern medicine and tracking techniques reduce the risk of more widespread epidemics, the modern, mobile world remains at risk for dangerous, possibly fatal contagious diseases. The plague killed millions during the middle ages; hundreds of thousands of people in this country died in the 1920's during an influenza epidemic. Recent events, such as the SARS crisis, remind us that these hazards continue to exist.

MAN-MADE HAZARDS

Fire

Building fire is one of the most common hazards. Every year fires cause thousands of deaths and billions of dollars in property damage. The National Safety Council estimated that in 1988 workplace fires caused over $3 billion dollars in damage and claimed 360 lives.



Hazardous Materials

Hazardous materials are substances that are either flammable or combustible, explosive, toxic, noxious, corrosive, oxidizable, an irritant or radioactive. A hazardous material release can pose a threat to life, health or property. Hazards can exist during production, storage, transportation, use or disposal. Hazardous materials are always nearby but do not necessarily have to be in the immediate vicinity in order to pose a great threat to life and safety.

TECHNOLOGICAL HAZARDS

Technological Emergencies

Technological emergencies include any interruption or loss of utility service, power source, life support system, information system or equipment needed to keep a organization in operation.

Power Service Disruption

Power service disruption could be the result of outside events such as an accident, power grid failure, weather or terrorism, or result from some internal problem. Power failures can have cascading effects, often disrupting other critical systems such as computer networks and communications systems. Depending on the nature of an operation, disruption in the delivery of other utility services could also constitute a major hazard for continued operations.

Environment Health

While outdoor air quality remains a major problem and can be an extraordinary hazard in some locations, indoor air quality has also become a great concern, both for affected organizations and the insurance industry. Primary threats to indoor air quality will include mold. Mold exists almost everywhere and people are exposed to it daily by touching, eating and breathing. In some cases, however, building conditions cause excessive growth of mold, which has adverse health consequences such as skin irritation, allergic reactions, asthma, headache and fatigue. Mold can also cause physical damage to buildings and building contents.

CRIMINAL AND TERRORISM HAZARDS

Terrorism

Terrorism is the threat or use of force or violence against persons or property for the purposes of intimidation, coercion or ransom. The goal is to create fear among the public, erode citizens' confidence in their government and to obtain immediate publicity for a cause. Although typically associated with political causes, terrorism may also be motivated by non-political reasons such as extortion and revenge.

Bomb Threats

Bomb threats can be a form of terrorism or someone's idea of a prank. In either case the results are the same and appropriate precautions must be taken.

Building Explosion

Explosions in buildings are most frequently caused by some internal malfunction or accident, however, in some instances the explosion is the result of a conscious attack. The results can be the same: immediate injury and death, damage to the building and its contents, fire and possibly collapse of the building.

Suspicious Letters and Parcels

Explosives and chemical or biological agents can be inserted into a facility through normal delivery channels. In some cases the letter, package or container may arouse enough suspicion that appropriate protective measures can be taken before the parcel is opened or has had the time to produce its intended consequences.

Chemical and Biological Weapons

Chemical agents designed for warfare may also be used as terrorist weapons. These agents are poisonous vapors, aerosols, liquids or solids that have toxic effects on people animals or plants. Some are odorless and tasteless. They can have an immediate effect or an effect that is delayed from hours to several days. Chemical agents tend to dissipate rapidly outdoors but can be very effective in a closed environment.

Cyber Attacks

Cyberterrorism is an attack on computers, networks and information systems. The most common type of attack uses software to infiltrate and damage an operating system or to perpetuate theft of information. Electronic systems are also vulnerable to physical attack through direct physical access to equipment and hardware or the use of electronic devices such as a High Energy Radio Frequency Gun or an Electromagnetic Pulse Transformer Bomb. Cyberterrorism is a particularly critical hazard for the telecommunications, finance and banking, electric power, and transportation industries.

Civil Unrest

Civil disturbances include riots, threatening individuals or assemblies that have become significantly disruptive. Demonstrations are actions designed to advocate a particular position on an issue. Most are peaceful and may only cause an inconvenience. They become a hazard when they disrupt operations.

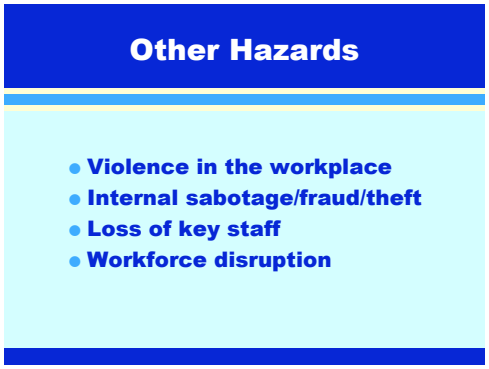
Robbery and Theft

Organizations dealing with the general public suffer the greatest exposure to the possibility of theft or being robbed. However, other businesses are not immune to robbery or theft and, depending upon the nature of the business, may be a target for larger and more sophisticated criminal endeavors.

OTHER HAZARDS

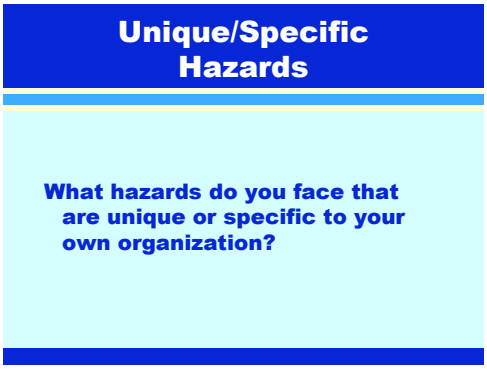
Violence in the Workplace

Violence in the workplace can be perpetuated by outsiders or by employees. In either case, many organizations have been found to be legally and financially responsible for the consequences.



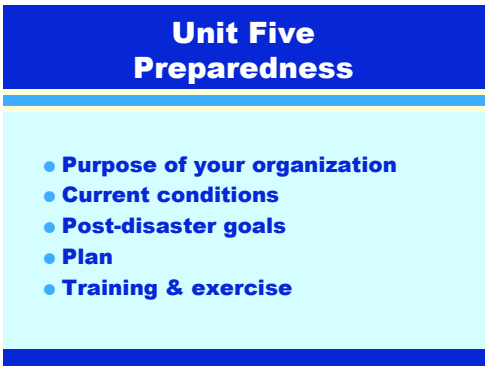
UNIQUE OR SPECIFIC HAZARDS

- What hazards do you face that are unique or specific to your own organization?



Unit Five
PREPAREDNESS

Preparedness is the process of making an organization ready and able to implement the other three phases of emergency management: response, recovery and mitigation. This Unit will focus on preparation, particularly the continued or on-going operation of your organization, that is, Continuity of Operations.

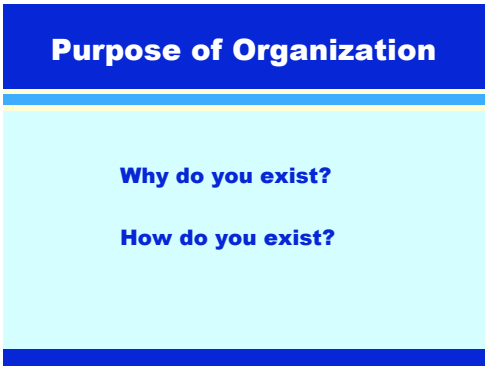


In order to know what you want to be and where you want to go after some disastrous event, you must first have a plan for getting there. And that plan begins with an understanding of who you are now and how today's operations function.

Prior to developing a Continuity of Operations plan three critical questions must be addressed. What is your purpose? What is your current condition? What is your goal? The answers to these questions will guide you and your team during the planning process as well as after any disaster.

PURPOSE OF ORGANIZATION

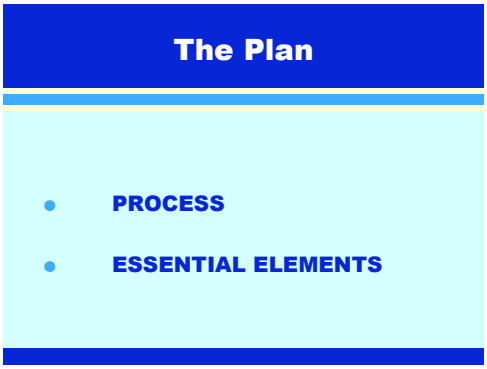
Why does your organization exist? What is its reason for being? As a business, the most likely reason is to generate a profit. How you generate that profit is the means to that end. A not-for-profit agency, by definition, has a different purpose. What is that purpose? Can it be accomplished in a manner different from the current model?



Essential Functions

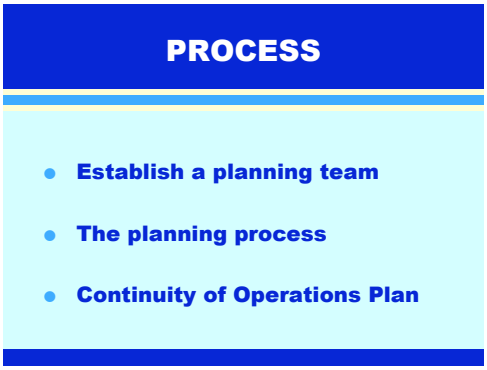
Having defined the purpose of your organization, it is necessary to understand the means by which these purposes are accomplished. What are your products and services? Who is involved (both internally and externally) in the achievement of your objectives? What facilities and equipment are needed? What administrative operations and personnel are vital to the operation? What are the necessary lifeline services such as utilities, transportation and communication? These "mission essential functions" are addressed more fully later in this unit.

THE PLAN



PROCESS

The Continuity of Operations plan cannot be predefined – no boilerplate, fill-in-the-blanks format will serve the unique needs of your particular organization. The process of developing the plan may be as valuable as the plan itself. Strong management support is critical to the success of the planning effort. Participation by all components of the organization is essential, both in the creation of the plan and, should it become necessary, in its post-disaster implementation.



Establish a Planning Team

The first step in the Continuity of Operations process is to create a planning team. This team is responsible for creating, implementing and maintaining the plan. The team approach will insure that all components and essential elements of your organization are represented in the process and are integrated into the plan. A team approach will also enhance the visibility and stature of the planning process throughout your organization, encourage participation in and commitment to that process and insure that sufficient time (manpower) is available to complete the task.

It is important that management strongly and visibly support the process. A policy statement should be issued by top management affirming the need for and value of the plan, while acknowledging the resources needed for its achievement. The statement should formally authorize the policy team to take the steps necessary to develop and implement the plan.

Finally, the management statement should appoint the members of the planning team. The team should be lead by the chief executive or a top-level manager. All functional areas should be represented.

Personnel should be selected based on their knowledge and skills. The team should include those who can be active members and those who can provide advice on specific components.

There should be one individual with overall responsibility for the planning process. Once the team is established, sub-committees based on the essential elements of the Continuity of Operations plan can be established. Other initial activities would include:

- Assignment of specific tasks
- Formation of an Emergency Management Action Team
- Creation of a work schedule and time-line for deliverables
- Development of a budget

The Planning Process

Prior to writing the plan, baseline information should be assembled by the planning team. An initial step would be to revisit the questions addressed by management prior to the creation of the team: what is the purpose of the organization and what are the essential functions? Additional information to be collected includes possible hazards/emergencies, vulnerability to these hazards and the organization's capacity to handle an emergency.

Current plans and policies that affect the process should be procured as well as building plans and site maps. Other baseline information would include: resource lists (equipment, supplies, services), hazardous materials (including cleaning supplies and chemicals), mutual aid agreements, security procedures, evacuation plans, information technology inventories and procedures, employee manuals, record retention procedures, organization charts and delegations of authority.

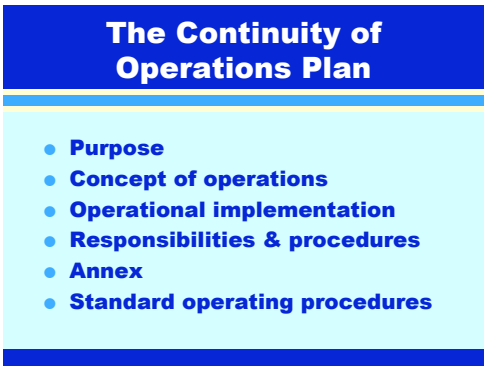
Codes and regulations affecting the organization's operations must also be identified. The team's legal advisers should identify hazardous materials rules, Occupational Safety & Health Administration (OSHA) regulations and other federal, state and local laws.

The steps in writing the plan are similar to most general planning processes. It is the focus of the plan, and the essential elements, that make it specific to Continuity of Operations. The general sequence is as follows:

- Establish goals
- Collect data
- Determine risks and vulnerabilities
- Analyze current capabilities
- Prepare first draft
- Internal review – across the organization
- Incorporate changes, prepare second draft
- External review – external parties affected by plan elements, outside experts, fellow agencies, state and local emergency management and other cognizant government agencies
- Incorporate changes, prepare final draft
- Final internal review – across the organization
- Present final plan to management for approval, official acceptance and adoption as company policy
- Print and distribute
- Train, exercise and regularly update

The Continuity of Operations Plan

The Continuity of Operations plan should address certain minimal "elements". These "elements" are described in greater detail later in this unit. Within each element and for the organization and plan as a whole there are various component parts that should be addressed. These include:



- Purpose, applicability and scope, and authorities and references

- Concept of Operations
  - * Key Staff
  - * Mission Essential Functions
  - * Direction and Control
  - * Alert and notification

- Operational implementation phases
  - * Activation
  - * Alternate Operations
  - * Recovery
  - * Termination

- Responsibilities and Procedures

- Annexes for each Essential Element

- Standard Operating Procedures, such as, but not limited to:

  - * Activation Procedures
  - * Notification Procedures
  - * Building Evacuation Plan
  - * Call Down Procedures and Lists
  - * Customer and Supplier Notification Plans
  - * Alternate Facilities Plans
  - * Site Support Procedures
  - * Resource Acquisition Plans
  - * Protection of Vital Records and Databases Plans
  - * Alternate Communications Plans
  - * Facility Disaster Supply Kit and Go Kit Checklists
  - * Family Preparedness Guidance

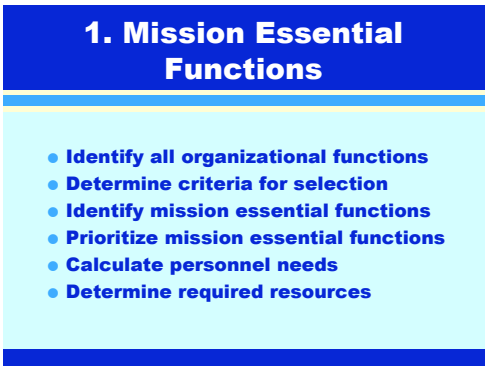
ESSENTIAL ELEMENTS

As noted above, a Continuity of Operations plan follows a generally accepted planning process, but contains certain components and elements that are essential to the plan's effectiveness and viability. The Essential Elements that will be found in a comprehensive Continuity of Operations plan include at a minimum:

1. Mission Essential Functions
2. Current Resources and Capabilities
3. Hazard Identification, Risk Assessment and Vulnerability
4. Delegation of Authority
5. Orders Succession
6. Logistics and Administration
7. Security
8. Communication
9. Facilities and Equipment
10. Vital Records / Information Technology
11. People
12. Supplies, Products and Services
13. Insurance
14. Community Interface

1. Mission Essential Functions

Mission essential functions are critical activities that are vital to the survival of the organization and the accomplishment of its mission. These functions must be performed or the organization ceases to operate. The identification of mission essential functions should be based on both the normal day-to-day operations and upon the responsibilities during a disaster.



Identify All Organizational Functions

- Operations
- Information Technology
- Legal
- Financial
- Administrative
- Planning
- Other

Tools and resources needed to carry out the function should be determined during the identification process. Do not overlook functions that may be small but are extremely significant. Do not group functions too broadly to be able to effectively describe the requisite support requirements. Do not group the functions in too much detail to be manageable. The Mission Essential Function list may be modified as information is developed in the planning process and in future versions as a result of data developed during the training and exercise phases.

Determine Criteria for Selection

Essential missions are those that must continue or the organization will fail. Not every important function or activity will be essential to the mission, however, it should not be assumed that those functions that do not appear on the essential mission list are unnecessary or superfluous to the organization's success. Designation as essential or non-essential should be based on the Continuity of Operations objectives and not reflect on the function's general contribution to the organization. This can be a very sensitive point and planners should be aware of the issue as they deal with the organization's personnel, sub-units and functional areas.

Identify Mission Essential Functions

- Apply selection criteria
- Would function increase, decrease, remain the same or terminate during an emergency?
- Would elimination or curtailment restrict the organization's ability to deliver its product or services?
- Be especially cautious of "single points of failure": functions where performance depends on a single resource or activity
- Determine organizational unit responsible for each function
- Identify organizational, product and service linkages to each essential function
- Identify resources necessary to keep the function operational

Prioritize Mission Essential Functions

Just as mission essential function identification is the result of prioritization of all organizational functions, prioritization with the mission essential function list is also necessary. Priority should be given to any function with life or safety issues. In some cases, one function may be the prerequisite for one or many other essential functions. Laws and regulations may mandate a certain priority.

- Determine which functions must be restored immediately or without interruption.
- Determine which functions are most critical to the organizational operations
- Rank in order of restoration

Identify Personnel Needs

Determine the manpower needed to perform the essential function. This may be based on a 24-hour operation divided into two or more shifts.

- Determine man-hours required
- Divide by shifts or operational hours to determine number of personnel required
- Assign personnel based on skill and knowledge
- Be certain that each assigned person is given the authority to perform the mission essential function

Determine Required Resources

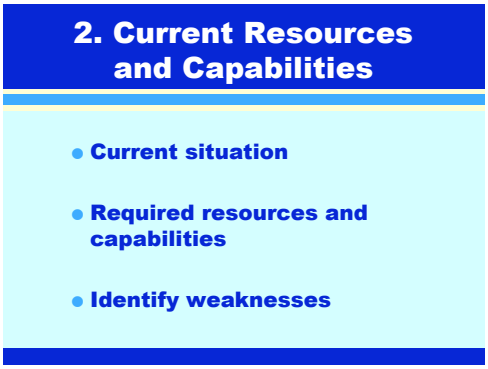
Each mission essential function should be examined to determine what, if any, special equipment or resources are necessary to carry out its objectives.

- Minimum information necessary to accomplish the function, including mission-specific information, vital records and Continuity of Operations plans, processes, checklists and standard operating procedures.
- Equipment, supplies, computer systems and software, communication systems, transportation and other resources required to accomplish the mission.

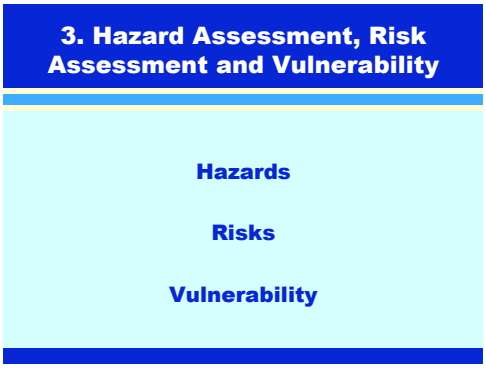
2. Current Resources and Capabilities

This essential element enables an organization to understand where it is now, what will be required to continue its operations and what capabilities and resources need to be developed in order to accomplish its essential missions.

- Analyze capabilities
- Inventory resources
- Examine organization charts and personnel assignments
- Evaluate lines of authority
- Review internal plans and policies
- Analyze lines of communication
- Determine weaknesses



3. Hazard Identification, Risk Assessment and Vulnerability



There are three concepts involved in considering the likelihood of an event adversely affecting your operations. "Hazard identification" consists of developing an understanding of the types of events that could affect you, your inter-organizational network or your community. Unit Four discussed potential hazards in some detail. As part of the Continuity of Operations planning process these hazards as well as others you might identify as unique or specific to your particular situation become the starting point for your analysis.

"Risk assessment" addresses the probability that a particular hazard might impact your organization, either directly or indirectly. It involves making the hazard specific to your planning process. Considerations might be location in a hurricane or flood zone, building construction, proximity to hazardous materials, historical events, or because of the nature of your product or service, the likelihood of terrorist or criminal activity. The range of possible hazards must be assessed to determine which are the greatest risks to you.

Finally, you must address the question of "vulnerability", that is, what is the potential impact on your organization. Vulnerability analysis examines the potential frequency and severity of an adverse event in terms of your organization's current capabilities as well as the length of time the event might impact you.

Vulnerability is frequently divided into three principal categories. Most important, of course, is human impact: your employees, customers and clients. You are considering the possibility of injury or even death. Safety issues will always be your top priority. Second to safety, but a part of the human impact are liability risks, potential damage to your reputation and business interruption.

Secondly, you must examine the vulnerability of your property, whether it be your facilities and equipment, supplies, stock and product, or such intangibles as your client lists, databases and other vital proprietary information. While some things can be repaired or replaced, others may not be replaceable. How vulnerable these items are and the cost-benefit of protective measures must be included in the analysis.

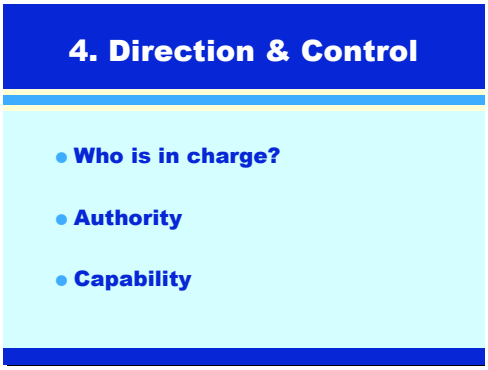
The vulnerability of your operations to an emergency must also be studied. Your organization can suffer great damage even if there are no life/safety issues and your property survives relatively unscathed. How vulnerable are you if your employees are unable to report to work, there is an interruption in critical supplies, the transportation distribution system is disrupted, or if utilities are unavailable?

Subsequent to assessing risks and vulnerabilities, it is important to assess you resources and ability to respond to each threat. Do you have the internal resources and capabilities to respond? Are there external resources available to respond or will they

have other priorities to serve? Can you establish mutual aid agreements? If the answers to these questions are no, you must then determine what can be done to prepare for the problem.[2]

4. Direction & Control

The Direction & Control element addresses how your agency is organized to direct the operations outlined in your Continuity of Operations plan. Someone must be in charge during an emergency. These procedures may differ dramatically from the normal day-to-day structure of your company operations, including most importantly, lines of authority. There are several types of organizational structures in use, including Emergency Support Function, Incident Command System and Emergency Management Group.



Whatever system is selected, the purpose is to develop a set of standard procedures for organizing personnel, facilities, equipment, supplies, services, communication and administration at the scene of an incident, which enables all parties to systematically organize and coordinate their efforts. This command system is responsible for front-line management of the incident, tactical planning and execution, determining whether outside assistance is needed, and for managing requests for internal and external resources

Such a system ensures safety, reduces confusion and further damage and allows critical decision-making within severe time limitations. It is implemented at the time the incident occurs and continues until the incident is closed. It can be expanded or reduced in size over the course of the incident as conditions demand, and can be used for small emergencies through major disasters.

[2] See Appendix 1

The emergency management team must have the capability and authority to:

- Assume command
- Assess the situation
- Implement the emergency management plan
- Determine and oversee response strategies
- Activate resources
- Order an evacuation
- Declare the incident "over"

5. Authority and Succession

After an incident has occurred, it is too late to determine who has the authority to do what. Authority, delegation of authority and lines of succession should be part of a normal course of business and are essential elements of a Continuity of Operations plan since roles and responsibilities will often differ during an emergency.

The plan should pre-delegate the authority required for making policy decisions and carrying out the responsibilities described in the plan. Document the necessary authorities, delineate the limits of authority and accountability and explicitly state the authority of designated successors. The plan should clearly state when the authorities become effective and when they terminate.

Orders of succession are also an essential element of the plan. In the event key leadership is unavailable, it is critical that responsibility and authority can rapidly transition in a stable and organized manner. Lines of succession should be pre-established, maintained and regularly updated.

At a minimum, delegations of authority and orders of succession should:

- Describe which authorities can and should be delegated
- Describe the circumstances under which the authorities would be exercised
- Specify when they would become effective and terminate
- Identify limitations of delegation
- Identify to whom authorities should be delegated
- Address conditions for succession
- Ensure the recipient of authority is prepared to execute the associated responsibilities

6. Logistics and Administration

This essential element of the plan provides for the administrative and logistical support of the response and recovery operations. Complete and accurate record keeping is a major function. Certain records may be required by law, some are necessary for insurance purposes and others may be invaluable in the event of any legal action. In addition, a detailed record of activities can become the basis for future plan revisions.

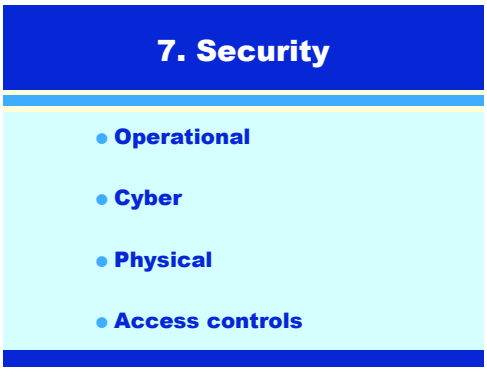
In addition to record keeping, a plan must be developed for the general administrative management of the operation, including personnel, purchasing, accounting, public relations and other functions that an administrative support team would normally provide.

The provision of equipment, supplies and services during an event will require logistical support. An analysis of what will be needed should be conducted in this element and provisions should be made to insure its availability. Outside assistance or mutual aid agreements may be considered. Service contracts, pre-positioning, off-site storage, and Go-Kits are possible alternatives. At a minimum the logistics portion of the plan should:

- Identify, pre-position and maintain equipment and other resources on-site and/or at off-site locations.
- Identify and arrange for the acquisition of equipment and other resources from outside sources
- Prepare and pre-position Go-Kits
- Provide for telecommunication and information technology support on-site and at any alternate facilities
- Establish provisions for personnel support, including food, lodging and transportation at all probable locations
- Provide for backup electrical power
- Prepare and maintain site support procedures for all necessary equipment, supplies and services

7. Security

Organizations should insure that all four types of security are addressed: Operational, Cyber, Physical, and Access Controls. Security measures for each of these areas should be incorporated into the Continuity of Operations plan.



Operational Security – measures to deny access to pieces of information that can be assembled to provide overall picture of your operation or a critical component.

Cyber Security – protection against access to information systems by unauthorized recipients and intentional but unauthorized destruction or alteration of that information system.

Physical Security – layering of physical barriers for site perimeter, protective lighting, and site surveillance, both overt and covert measures are used.

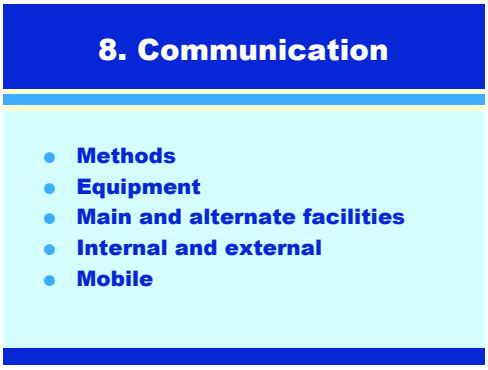
Access Controls– measures used to control access to facility or site: keys, ID cards, PINs, or other identifying techniques

Each organization should:

•Establish Operational Security and Cyber Guidelines, including guidelines for handling the Continuity of Operations plan
•Address physical security of current facilities and at alternate facilities
•Enact personnel access controls for employees and critical customers
•Address security of communications, if appropriate
•Be prepared to augment all security levels based on the emergency or the threat

8. Communication

The communications element of the plan should examine what methods and equipment will be needed to report emergencies, warn personnel and customers of danger, keep in contact with customers and suppliers, keep employees and families informed and coordinate response and recovery actions, keeping in mind that normal communications could be disrupted in many ways. The ability to communicate both at existing facilities and alternate facilities must be developed.



The communications capability should be commensurate with the organization's planned operations. Redundancy of communications is vital and the capability should be developed to sufficient depth to assure availability

Within the Continuity of Operations plan communications should at a minimum:

•Identify the data and communications systems needed to support mission essential functions
•Ensure availability at main and alternate facilities of
  –Voice and fax
  –Cellular
  –Satellite
  –Internet and email
  –Data systems
  –Emergency systems (NAWAS, EAS, etc), if necessary
  –Secure communications, if necessary
•Provide for both internal and external communications
•Consider mobile communications capabilities

9. Facilities & Equipment

Procedures for protecting facilities and equipment are essential to timely restoration of operations. The first step in this process is a physical inventory of all property. For planning purposes many items can be grouped if they warrant similar protective action, e.g., moving vehicles to a safe location. Examples of other procedures include:

- Fighting fires
- Containing hazardous materials spills
- Shutting down utilities
- Shutting down equipment
- Closing and/or covering doors and windows
- Covering and/or securing equipment and supplies
- Moving equipment to a safe location

This element of the plan should also examine the need for pre-installed protective systems such as:

- Fire protection systems, including monitoring, warning and extinguishing
- Lightning protection
- Water-level monitoring
- Overflow detection devices
- Emergency power
- Security systems

In some cases your efforts to protect your facilities and equipment will be inadequate. You may find that your building will be inaccessible for 48 hours, or 72 hours or a week. Following a hurricane or other major disaster, you may not be able to reopen your facility for weeks or even months. How will you be able to operate?

The answer is to have plans in place to use an alternate facility. This element of the Continuity of Operations plan should identify an alternate operating facility or facilities, as needed. The facility should be capable of accommodating and supporting all mission essential operations for a minimum of 30 days. At a minimum, the plan should:

- Identify potential sites from existing organization facilities, if available
- Consider cooperative agreements, sharing with other organizations and virtual office technologies
- Ensure sufficient space and equipment is available to accommodate a defined number of relocating personnel and any specialized equipment that must be brought in to the facility
- Provide for reliable logistical support, services, and infrastructure systems
- Ensure the ability to sustain operations for a period of up to 30 days
- Consider pre-positioning assets and resources at proposed facility
- Ensure appropriate physical security and access controls

10. Vital Records and Databases

The Continuity of Operations plan should provide for the protection and availability of electronic and hardcopy (as applicable) mission essential records, documents, references, information systems and databases. These vital records may include, but not be limited to, financial and insurance information, engineering plans and drawings, product lists and specifications, employee, customer and supplier databases, personnel files, corporate and legal records, and formulas and trade secrets.[3]

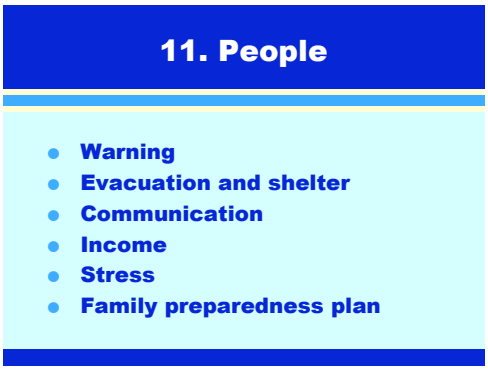
At a minimum the plan should:

- Identify vital records, systems and data (hard copy and electronic) that are critical to mission essential functions
  - * Classify operations into functional categories (finance, research, administration, etc.)
  - * Determine mission essential functions
  - * Identify minimum information that must be preserved and available
  - * Identify the records that contain this essential information
  - * Identify the equipment and materials needed to access and use the information

[3] See Appendices 11, 12, 13, 14, 15, 16

- Plan for the protection, duplication, movement and storage of records, such as
    * Labeling vital records
    * Backing up computer systems
    * Making hard copies
    * Converting hard copies to electronic files
    * Storing in secure/safe rooms
    * Storing at various off-site locations
    * Increasing security of computer equipment
    * Arranging for evacuation of records to alternate or backup facilities
    * Arranging for backup power
- Ensure accuracy and currency of records by having a regular updating plan
- Ensure procedures for creation and maintenance of new records created during and after an incident, including accurate records of response and recovery operations

11. People



One element of the plan should specifically address the needs of people, particularly organization personnel. The safety of all persons occupying a facility at the onset of an incident is paramount. This implies the need for a warning system, evacuation procedures and/or in-house sheltering.

Warning systems should be audible/viewable by all people in the facility and have an auxiliary power supply. Procedures should be established to warn customers and outsiders who may not be familiar with the system. Test the system regularly.

Evacuation plans include clear lines of authority and management, routing and assembly, operational shutdown and re-entry procedures.[4] In some cases the best means of protection is taking shelter within the facility. In this case secure space must be identified and equipped with the appropriate supplies, equipment, food and water. A system should also be designed to manage the operation and the shelter.

Employees, as well as those who will be responsible for implementing the plans, should be trained in these emergency protective procedures. Evacuation and sheltering procedures should be provided in writing and the necessary maps and other guidance posted in strategic locations. Regular drills are imperative.

[4] See Appendices 18 & 19

Survival of an organization during and after an emergency will depend as much as anything on the well-being and survival of its personnel. It is in the best interest of the organization to provide as much employee support as possible. This support can take a variety of forms, depending on the nature of the emergency, the needs of the employees and the capacity of the organization.

A part of any personnel support plan, however, is communication with the employees. Basic information concerning the impact of the emergency on the organization, current activities and immediate plans are essential to the employee. How this information is to be disseminated should be established. Inform the employees how and when they may call in. Establish and continually update employee and management rosters. Create call down lists or telephone trees.[5]

Equally important, employees who remain at the facility will need to know if their families are safe (or they will probably leave). All employees should be encouraged to consider how they would communicate with their family if they were separated from one another. In addition to direct contact, they can arrange to communicate through a third party who lives out of the area. In case their home is impacted, emergency meeting places can be pre-determined.

Payroll is an extremely important issue to employees. Computers may be down, power could be interrupted and banks and ATM's may be out of service. Employees may need to make repairs, take care of everyday needs and report to work. Plans and backup plans need to be developed to insure that employees can be paid.

Additionally, your operation may be shut down or be on reduced hours. In this time of need, is it possible to provide pay advances for those employees who are not working?

If the emergency is widespread, employees may need flexibility and support from management in order to take care of added personal responsibilities. Could work-at-home, reduced hours or flexible hours be made available?

An emergency can create enormous amounts of stress. This stress can be created both as a result of conditions at the organization and because of conditions at home. When developing an emergency management team, training managers to recognize and deal with stress is a valuable investment. The return to normal operations will be enhanced if stress is acknowledged as one of the impediments to recovery.

Stress is an inevitable part of the recovery process for all personnel, including not only staff, but leadership and management (maybe even more so) as well. It would be wise to consider the possibility of developing crisis counseling teams or employing stress management professionals to assist in handling these needs.

[5] See Appendix 8

Employee Family Preparedness

Employees will be extremely concerned about their own personal safety, that of their families and their homes during an emergency. If they have no plan to deal with the personal effects of the emergency, it is unlikely they will be able to be of much assistance in the organization's response to events.

Employees should be encouraged to create their own emergency preparedness plan. At a minimum the plan should address the following issues:

- Advance arrangements for property and contents protection
- Food, water, supply and medicine cache
- Alternate shelter options in the event of evacuation.
- Evacuation plans and checklists
- Family communication procedures
- Knowledge of flood zones, evacuation zones, geographic conditions
- Dependent care
- Medical/dental: Medical records, prescriptions and supplies, location of emergency service providers
- Cash and other resources
- Pet care
- Transportation and fuel

There are numerous sources of guidance for the preparation of a family preparedness plan, particularly the American Red Cross, Florida Division of Emergency Management and the Federal Emergency Management Agency.[6]

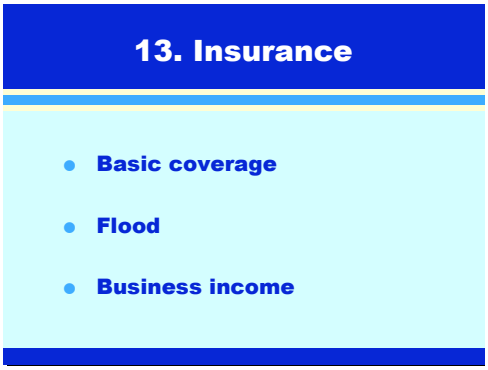
12. Supplies, Products and Services

The core of your operation is the delivery of a product or a service. To produce a product or service you must obtain supplies and services. If this chain of activity is interrupted, your operation is also interrupted, or even shut down. This essential element of your plan should address how to maintain your supply of goods and services, how to protect your existing inventory of supplies and products and how to continue to deliver your service to your customers.

[6] See Appendix 20

13. Insurance

Insurance provides the financial means to recover from disasters and other large or small events that can adversely affect your organization. Your best source for information will be your insurance agent. Appendix 3, the Insurance Coverage Discussion Form, is a useful tool to help you get started. Following is a very brief overview of the types of insurance that you should consider when developing your Continuity of Operations plan.



- Property - covers physical assets such as buildings, equipment, furnishings, inventory and more. In some cases it may also provide income if your agency is forced to suspend operations after a covered loss.

- Liability – designed to protect your organizational assets if you are sued for something you did or didn't do that resulted in bodily harm or property damage to someone else.

  Many insurance providers bundle property and liability insurance coverage into a owner's policy. The basic package can then be tailored to your specific needs, including adding other coverages such as lost income.

- Flood – you are four times more likely to experience a flood than a fire. Yet most property insurance policies do not cover damage from flooding. A separate flood insurance policy should be considered and certainly should be purchased if you are in an area that has any possibility of flooding. Your insurance agent or local government can help you access information on the flooding potential of your location.

- Commercial Automobile – your personal automobile insurance policy will not cover you when the vehicle is being used for your organization. A commercial policy is necessary. You may also want to consider coverage for "non-owned" vehicles: when employees use their own vehicles for company purposes or when your agency uses rental vehicles.

- Workman's Compensation – required by law in most states, this type of insurance provides benefits to employees who suffer some job-related injury or illness. In addition, Employer's Liability Coverage protects employers in the event they are sued for damages arising from employment-related injury or disease.

- Errors & Omissions – this type of policy covers your financial exposure if you are sued in the course of your business for failing to provide correct information or advice or for providing incorrect information or advice.

- Umbrella – provides additional liability insurance coverage after the limits of your basic policy have been reached.

14. Community Relations

Your organization is part of a broader community. Your relationship with the community will influence the success of your current operation as well as your ability to protect personnel and property and return to normal operations after an emergency. This important element of your Continuity of Operations plan should focus on your interaction with your customers, other organizations, the media and the general public.

- Maintain a dialogue with community leaders, first responders, government agencies, community organizations and utilities. Involve appropriate agencies in the development of your plan and have them participate in exercises. Meet with community groups and conduct facility tours. Be a part of the community.

- Establish mutual aid agreements with local response agencies.

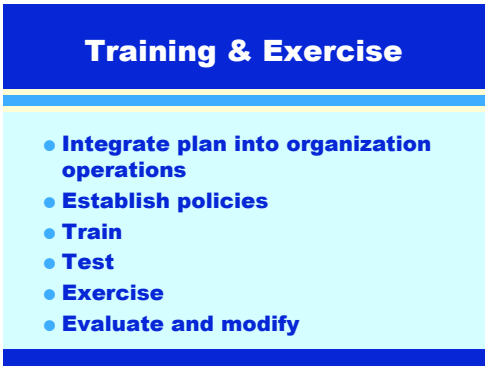
- Look for opportunities to provide community service, before and during emergencies: sheltering, personnel, equipment, transportation, product.

- Have a public information plan in place: suppliers, customers, shareholders, neighbors, emergency organizations, regulatory agencies, and the general public.

- Plan, develop and staff a media relations program. Do not wait for an event to occur. Make this activity a distinct component of the overall planning process.

TRAINING AND EXERCISE

Train • Test • Exercise • Modify



In order to implement the Continuity of Operations plan, you must integrate it into company operations, train your personnel, test their skills and exercise the procedures. Lessons learned in the process will allow you to correct, modify and refine the Continuity of Operations plan.

A written plan is just a starting point. Turning it into a dependable, effective activity takes additional work. Training your personnel permits them to be confident in their roles. Testing and exercise helps to develop expertise and allows the planners to evaluate the effectiveness of the various components.

A comprehensive training and exercise program should:

- Integrate the plan into agency operations
- Establish policy guidance and standards
- Include training courses and materials
- Contain regularly scheduled tests
- Involve exercises of various types and complexity
- Include evaluations and remedial action processes

Integrate the Plan

- Insure that senior management supports the plan and knows their own roles in its execution
- Fully incorporate the plan into the company's accounting, personnel and financial procedures, including specific and adequate budget allocations
- Integrate all levels of the organization, including regions and field locations
- Develop annual, company-wide testing, training and exercise schedules[7]
- Involve all levels of the organization in plan evaluation and modification

Establish Policy Guidance and Standards

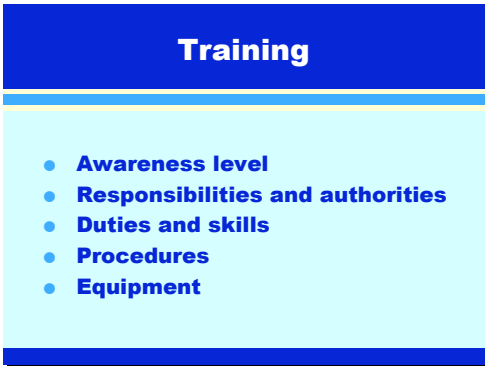
[7] See Appendix 2

- Develop a formal training and exercise program
- Establish a working advisory group
- Assign specific responsibility to one person, with the option of additional staff as necessary
- Determine:

    * What will be trained and exercised
    * Who will be trained and exercised
    * Who will conduct the training and exercises
    * When, were and how frequent the activities will occur
    * Who will evaluate the training and exercises
    * A budget

Training

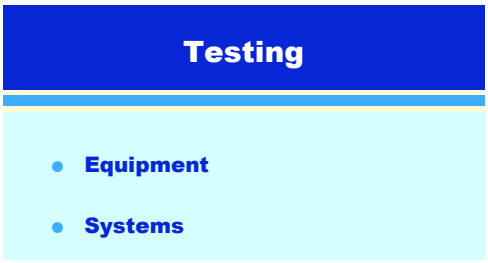
The purpose of training is to prepare organization personnel to institute emergency operations, possibility at an alternate site, to use equipment and procedures described in the Continuity of Operations plan and to work with individuals with whom they may have little contact on a day-to-day basis. The length and complexity of the training will vary depending on the audience and specific training topics. Major topics of a training curriculum could include:



- Continuity of Operations awareness and overview
- Systems of Direction and Control
- Preparedness for managers and key decision-makers
- Essential Elements as a group and/or individually
- Major operational elements
- Notification and warning
- Evacuation and sheltering
- Threats, hazards and protective actions
- Emergency shutdown procedures
- Operations at a remote facility
- Operation of equipment
- Communications equipment and procedures
- Roles and responsibilities for specific assignments
- Personal and family emergency plans

Testing

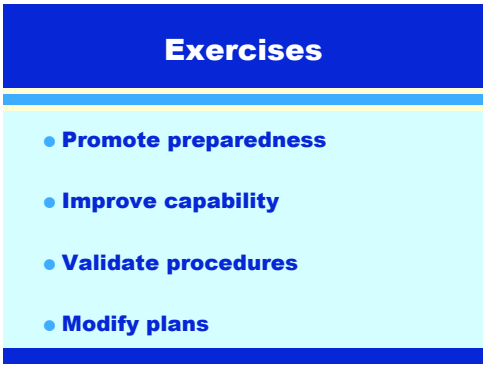
The organization should regularly test equipment, systems, processes and procedures to insure the equipment and



systems conform to specifications, operate in the required environments and viable. Testing should include backup equipment and systems as well as primary systems and equipment. Tests should be performed frequently enough to insure that current personnel have retained operational knowledge and that new personnel are capable of operating the equipment or system. Particular attention should be given to:

- Alert and notification systems and procedures
- Communication systems and equipment
- Vital records, data management, computer hardware and software
- Logistical support, including procedures, equipment and services.

Exercise



An exercise should be a realistic rehearsal or simulation of an emergency, in which individuals and organizations demonstrate the tasks that would be expected of them in a real emergency. The purpose of an exercise is to validate elements, both individually and collectively, of the organization's Continuity of Operations plan. Exercises should provide emergency simulations that promote preparedness, improve the response capability of individuals and organizations, and validate plans and procedures. Each organization should schedule regular exercises of their Continuity of Operation plans. The exercise program should:

•Consist of a variety of potential hazards
•Incorporate deployment of personnel to alternate facility
•Provide for continuation of operations through all phases of an event
•Include participation at multiple levels and provide for interaction with Federal and local governments when applicable

Exercises may vary in size and complexity to achieve their respective purposes. Examples of emergency exercises include:

- Tabletop Exercise – discussion of emergency responsibilities and actions in response to a theoretical emergency in an informal, conference-like setting.

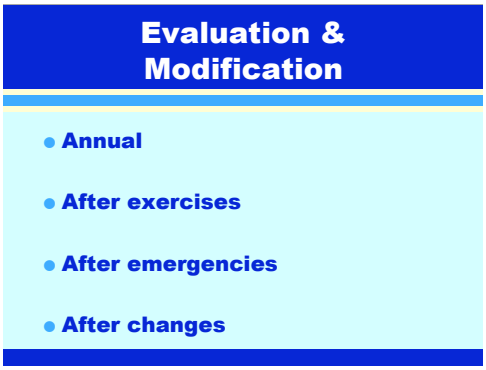
- Walk-through Drill – more thorough than a tabletop exercise, this drill usually tests a single specific operation or function. The walk-through aspect usually incorporates frequent pauses for discussion, additional training and interim evaluation.

- Functional Drill or Exercise – usually tests an entire function, such as emergency notification, warning and communication or vital records management. These drills and exercises tend to be more realistic, with evaluation occurring after the completion of the activity.

- Full-scale Exercise – a real-life emergency situation is simulated and the entire emergency plan is activated and tested, with (in most cases) the entire organization participating. Third parties frequently evaluate full-scale exercises and the evaluation process can be quite formal and extensive.

Evaluation & Modification

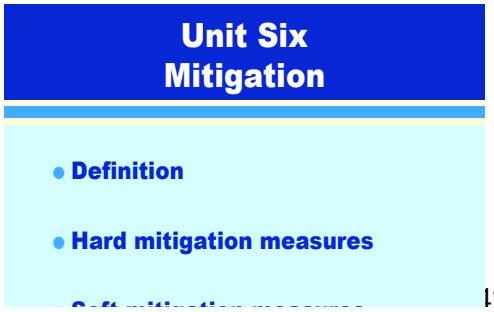
The Continuity of Operations plan should be continuously reevaluated. Certain elements work well, others not as well. Personnel change, your operation evolves, buildings are remodeled, equipment and systems are modified. New equipment and procedures become available. Organizations should analyze, and modify their plan as necessary, on a regular basis:



- A thorough annual review of the entire plan
- After each drill or exercise
- After any emergency
- When personnel or their responsibilities change
- When the layout or design of the facilities changes
- When policies or procedures change
- When any other event occurs that may significantly impact the effectiveness of the plan

Unit Six
MITIGATION

While the other three phases of emergency management address how to prepare for, respond to or recover from an emergency or disaster, mitigation is concerned with



minimizing or avoiding hazards and their consequences in the first place. Mitigation is a prevention strategy. It consists of preventive measures taken to eliminate or reduce the risk of experiencing an emergency, decrease vulnerability and minimize potential damage and other adverse consequences. Mitigation actions are those steps that you can take now to short-circuit an emergency before it occurs.

Mitigation falls into two broad categories. Soft mitigation measures often have wide application and benefits and tend to be processes and procedures, such as

- Plans, e.g. a Continuality of Operations plan
- Organizational
- Rules and regulations, e.g., hazardous material handling, no smoking, land use
- Insurance

Hard mitigation generally applies to physical measures and structural items. Examples include:

- Incorporating protective measures into new construction
- Installing hurricane shutters
- Building retention ponds
- Moving vulnerable equipment and supplies to a more protected location
- Acquiring emergency equipment and supplies

Following is a sampling of mitigation measures that might be applicable to some of the hazards discussed in Unit Four.

Possible Mitigation Measures

- **Building fire**
- **Wildfire**
- **Hurricanes & other windstorms**
- **Flooding**
- **Agricultural diseases and pests**

Building Fire[8]

- Inspect facilities and seek fire prevention recommendations from local fire department and insurance carrier
- Build fire exits and develop an evacuation plan
- Install smoke alarms, warning systems and fire extinguishers

[8] See Appendices 32 & 33

- Install sprinkler systems, fire hoses and fire resistant doors and walls
- Establish procedures for safe handling of flammable material and debris
- Identify and label all utility cutoffs so that they can be quickly shut off by fire fighters and other responding personnel
- Properly maintain and regularly inspect all heat producing equipment

Wildfire

- Clear brush and trees at least thirty feet back from any facility
- Preferably keep the cleared area around a facility at a width greater than the height of the nearest trees
- Insure that emergency vehicles can reach facility by providing well-marked access points, and access roads at least twelve feet wide with sufficient turn-around space
- Construct structures, especially roofs, of fire resistant material
- Insure that water sources are available in the form of hydrants, storage tanks, ponds or wells

Hurricanes and Other Windstorms[9]

- Establish facility shutdown and evacuation procedures
- Develop plans to protect vital records, communication systems and computer networks
- Prepare Disaster Supply Kits[10] and Disaster Go-Kits[11]

- Conduct a structural survey of facilities and make improvements necessary to meet recommended wind load requirements
- Install hurricane shutters on doors and windows or take other steps to harden openings in the building envelope
- Acquire a back-up generator

Flooding[12]

- Determine if your facility is in a flood hazard zone
- Purchase flood insurance
- Construct barriers such as levees, berms and floodwalls to prevent flood water from entering facility
- Elevate or move flood prone buildings
- Seal below-grade walls to prevent seepage
- Insure all stormwater infrastructure is of adequate design capacity, clear of debris and properly functioning

[9] See Appendices 21 &23
[10] See Appendix 9
[11] See Appendix 10
[12] See Appendix 22

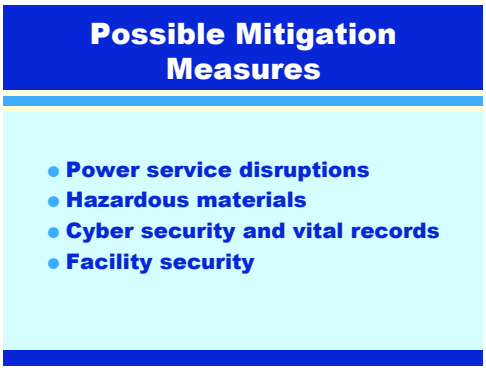
- Install check valves or other devices to prevent backflow through drainage, sanitary sewer and other utility access systems

Agricultural Diseases and Pests

- Develop a regular surveillance system
- Have plans in place to obtain rapid diagnosis of potential problems
- Maintain an ongoing program of disease and pest prevention
- Keep vehicles and non-business visitors away from animals and crops
- Isolate new animals before allowing them to join existing stock
- For information on agricultural terrorism see Appendix 30

Power Service Disruption

- Acquire uninterruptible battery backup equipment for computers and other critical equipment
- Install surge protectors
- Install battery powered security and backup lighting systems
- Obtain or pre-plan for the acquisition, installation and operation of a generator



Hazardous Materials[13]

- Work with the Local Emergency Planning Committee in developing site and community warning systems and evacuation plans
- Identify and label all hazardous material handled, produced or disposed of in the facility
- Acquire equipment necessary to contain, neutralize and clean up known hazardous materials
- Store all dangerous materials in secure facilities
- Organized and train an emergency response team to confine and control hazardous material

Cyber Security and Vital Records[14]

- Purchase, keep up-to-date, and use various software programs such a fire walls and virus protection
- Physically secure computing areas and equipment
- Scan paper records
- As necessary, encrypt valuable or sensitive data
- Store duplicate records and electronic data off-site, preferably out of the area but in equally secure conditions
- Shred or destroy out-dated records
- Establish secure procedures for disposing of old disks and hard drives
- Permit only authorized, badged, employees to have access to sensitive records and computer areas

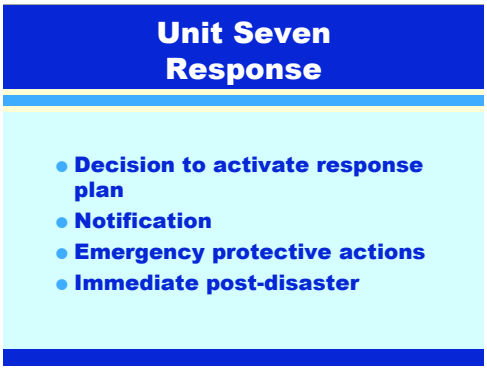
Facility Security

- Work with local law enforcement officials in developing a security plan
- Complete a thorough background check before hiring any new employee
- Develop access controls to prevent non-employees from entering the non-public areas of the facility
- Create an employee identification system such as badges
- Insure that all opening can be properly secured and that procedures are in place to verify that they are locked
- Install security cameras
- Install adequate lighting, both indoors and on the facility grounds
- Acquire locking cabinets, safes or vaults for the storage of more sensitive or valuable information, equipment and goods

[13] See Appendices 31 & 36
[14] See Appendices 14, 15, 16,17

Unit Seven
RESPONSE

Response is that phase of the emergency management cycle that occurs immediately before, during, and immediately after an emergency event. It is not merely a reaction; it is a planned set of operations designed, to the extent possible, to manage and control the event and its consequences.



DECISION TO ACTIVATE RESPONSE PLAN

The first step in the response phase is to activate the response plan. If the emergency has been identified as a pending event, such as a hurricane or expected flooding, senior management and Emergency Management Group leaders will have time to assess the situation. The need to launch the plan can be considered, appropriate activation schedules developed and notifications issued. If the emergency is a sudden event such as a fire or explosion, some elements of the planned response (e.g., evacuation) will be carried out automatically. Issuance of a formal statement converting from normal operations to an emergency management mode may lag actual events for a while.

In both cases, however, authorized leadership will have to make a decision to activate the plan and go into the response mode. After authorization, the various plan elements could then start their response activities. If time permits, pre-event preparation would begin immediately. Implementation of other plan elements would be scheduled, but some elements would promptly commence emergency operations.

NOTIFICATION

Once the plan is put into action the first step in the process is notification. Required emergency warnings should be issued and, as necessary, alarm systems activated. The Emergency Management Group should be informed of plan activation and immediately assume their assigned roles. Any gaps in the Emergency Management Group roster should be filled and initial work schedules posted.

Notification should be given to all facility occupants and to off-site employees. Written and pre-addressed “blast faxes” and grouped email messages can provide accurate information to a wide audience within minutes. Telephone trees or call-down lists are another means of notification. The media relations team should be an integral part of this process.

EMERGENCY PROTECTIVE ACTIONS

The protection of employees and visitors becomes a first priority. The decision whether to shelter in place or to evacuate must be made as rapidly as possible, in some cases immediately.

The shutdown of normal operations should be quickly decided and initiated if necessary. Building and equipment protective measures should be started, such as:

- Sandbagging
- Securing/covering/evacuating equipment
- Utility cutoffs
- Covering windows and doors

In accordance with the response plan and as appropriate to the specific emergency, the other functional elements of the plan should be initiated using plan checklists, procedures and guidelines.

IMMEDIATE POST-EMERGENCY

Response processes will continue in the immediate aftermath of an event, even as the recovery phase gets underway. Depending on the magnitude of the emergency and the impact on the organization's facilities and operations, response could continue for a few days to a week or two.

The first post-emergency response function is to address human life and safety issues. Immediately account for all occupants of the facility and assess their status. As necessary, initiate search and rescue operations and tend to the injured.

Simultaneously, designated teams should commence damage control, for example, put out fires or cover leaking roofs. Once the facility has been secured against further damage, the response team should conduct an initial damage assessment. This assessment differs from the detailed quantification of damage that the recovery team will conduct. Rather, it should be an overall assessment of the situation that the Emergency Management Group will use to guide its decisions as it directs the response and recovery process.

This brief overview is not intended to be an exhaustive description of the entire response phase. Rather, it highlights the initial steps in the response process, recognizing that the full details of a response operation will be contained in the organization's Continuity of Operations plan.

Unit Eight

RECOVERY

The recovery phase of emergency management consists of restoring the physical and operational elements of an organization to their pre-disaster state. It may include modified, improved or alternative solutions.

IMPLEMENT THE PLAN

The emergency has passed. The Continuity of Operations plan has been activated. Your people have been taken care of and the facility has been secured against further damage. It is now time for the recovery section to take the steps necessary to minimize any interruption in business and restore the organization to full operational capability.

Recovery activities are defined in the Continuity of Operations plan and should be scheduled and executed using the checklists, procedures and guidelines contained in this valuable document. Gather the recovery team together and set up the base of operations as soon as possible. All team members may not be available. Fill in any gaps in the roster and assure that lines of succession and chains of command are in order.

Initial recovery activities, some of which may be pursued in concert with the response group, include:

- Temporary repairs to facilities and equipment
- Clean up
- Taking measures necessary to assure the safety of building occupants
- Restoring utility service
- Implementing new security procedures
- Quantitative physical damage assessment
- Photographing and/or videotaping facility for documentation of damage
- Determining need to move to an alternate location
- Considering need to contract for post-emergency services, supplies or equipment
- Meeting with insurance agent and claims adjusters
- Analyzing damage to agency operations
- Restoring essential agency functions
- Contacting suppliers and customers
- Keeping accurate records of emergency activities and expenditures

PERIODS OF RECOVERY

Depending on the severity of the emergency and the degree of impact on your organization, the recovery period may last for quite a long time. Recovery is usually viewed as having three overlapping time periods:

- Immediate Emergency Period
- Short Term Restoration
- Long Term Reconstruction

The actual length of any recovery period will vary based on many factors. Obviously, the amount of damage your organization has experienced will affect how long it takes to get back to normal operations. But there is also the question of how widespread the damage is in the community. Area transportation and utility systems may be destroyed. Competition for goods and services may make it difficult to pursue some recovery options. Your suppliers and customers may have been severely impacted.

Positively affecting the length of time it takes to recover, however, will be the Continuity of Operations plan. While others are floundering, your organization will have an action plan with specific steps to orchestrate the recovery process. Your expert recovery team, having been trained in its duties, with skills polished through exercises, will make a huge difference in the time it takes to restore facilities and return the organization's operations to normal.

IMMEDIATE EMERGENCY PERIOD

During the Immediate Emergency Period most of the activity will be conducted by response personnel as they manage the event and attempt to stabilize the situation. For the most part, the recovery team will be organizing and setting up operations during this period, which lasts for a few days and usually no longer than the first week.

During this time period you may experience access or re-entry obstacles. If there is widespread damage in the area, roads may not be passable, lives wires could be on the ground and there could be curfews due to security issues. The organization's facilities could be inaccessible for similar reasons of safety and security. In cases of fire or suspicious events, law enforcement authorities may limit access to a site.

This is a time to be patient. It may be several days before access is available. There is recovery work to do that does not necessitate a presence at the organization's facilities. If personnel can communicate by telephone or other means, or move about the community, there are many recovery tasks that can be initiated without going to the organization's facilities.

SHORT TERM RESTORATION

Beginning a few days to a week after an emergency and extending for some weeks thereafter, the Short Term Restoration Period will see the recovery team focusing on activities that can be quickly normalized, while at the same time organizing for those that require a longer term commitment. The Short Term Restoration actions will include minor repairs, cleanup and disposition of debris, salvage operations, restoration of utilities and damage assessment. Reinstitution of operations, including restoration of vital records, computer systems and communication systems will be a high priority.

In addition to the repair and restoration tasks, during the Short Term Restoration period recovery personnel will be directing broader emergency management functions such as crisis communication, employee support, security, logistics and administration.

Dealing with the organization's insurance carrier will require substantial time and effort during this period. Contact your agent as soon as possible after the emergency. Remember that in a widespread emergency the agent will be overwhelmed and may not be immediately available. In major emergencies, outside claims adjusters are brought in, but even that takes some time to establish.

Photograph or videotape the condition of the facility and its contents before cleanup and repairs are started. Keep meticulous records of all costs associated with the emergency. Commence documentation of income or related losses.

LONG TERM RECONSTRUCTION

The Long Term Reconstruction Period starts a few weeks after the emergency and continues until rebuilding is complete and the organization is operating at pre-emergency levels. This could be a few weeks or months but in some cases it could take years. During the Long Term Reconstruction Period the Short Term Restoration activities should continue until completed. Those functions not directly associated with restoration, such as employee support and crisis communications would operate throughout the entire Long Term Reconstruction Period.

The Long Term Reconstruction Period involves those challenges that take greater time because of their magnitude and complexity. Large demolition projects can be complex and time-consuming. Major construction or reconstruction takes time to plan, engineer, fund, contract, permit and build. When the entire community is in the recovery mode competition for services and materials will add more time to reconstruction schedules.

Funding for reconstruction may come from several sources. The first line of defense is adequate insurance. Except that insurance is not always adequate, some costs may not be covered and there are always deductibles to consider.

Unit Nine
ADDITIONAL RESOURCES

Literature

Source material for this Guide

Continuity of Operations: Elements of Viability, Introduction to Continuity of Operations (COOP) and Continuity of Government (COG), Course Participant Workbook
Karen C. Delimater
Florida Division of Emergency Management

Emergency Management Guide for Business & Industry: A Step-By-Step Approach to Emergency Planning, Response and Recovery for Companies of All Sizes
Federal Emergency Management Agency, 1993

Emergency Preparedness Information (CD)
Ocala-Marion County Economic Development Corporation and the Institute for Business and Home Safety, 2001

Florida Business Disaster Survival Kit, Business Continuity Planning in Today's World
Tampa Bay Regional Planning Council and the Business Continuity Planning Alliance in association with the State of Florida Division of Emergency Management and the Florida Regional Planning Councils, 2003

Florida Business Disaster Survival Kit, Business Continuity Planning in Today's World (CD)
Tampa Bay Regional Planning Council and the Business Continuity Planning Alliance in association with the State of Florida Division of Emergency Management and the Florida Regional Planning Councils, 2003

Open for Business, A Disaster Toolkit for the Small Business Owner
Institute for Business & Home Safety, ©1999

Organizations At Risk: What Happens When Small Businesses and Not-For-Profits Encounter Natural Disasters
David J. Alesch, James N. Holly, Elliott Mittler and Robert Nagy
University of Wisconsin-Green Bay Center for Organizational Studies, 2001

Additional Literature

Business Emergency Action Plan, Edmond D. Jones, MBCP,
Rothstein Associates, Inc., 2001

Business Threat and Risk Assessment Checklist, Edmond D. Jones, MBCP,
Rothstein Associates, Inc., 2001

Continuity Planning and Disaster Recovery: A Small Business Guide
Donna R. Childs & Stefan Dietrich, 2002

Disaster Mitigation Guide for Business and Industry (FEMA 190)
Federal Emergency Management Agency

Emergency and Disaster Planning Manual, Laura G. Kaplan, 1996

NFPA 232: Standard for the Protection of Records, National Fire Protection Association, 2000

NFPA 1600: Standard Disaster Emergency Management And Business Continuity Programs, National Fire Protection Association, 2000

Unforeseen Circumstances: Strategies & Technologies for Protecting Your Business & Your People in a Less Secure World, Alexis D. Gutzman, 2002

Organizations

Association of Contingency Planners International
7044 South 13th Street
Oak Creek, WI 53154
1-800-445-4227
http://acp-international.com/

Department of Commerce
Economic Development Administration
Herbert C. Hoover Building
Washington, DC 20230
202-482-2659
http://12.39.209.165/xp/EDAPublic/Home/EDAHomePage.xml

Federal Emergency Management Agency
500 C Street, S.W.
Washington, D.C. 20472
1-800-480-2520
www.fema.gov

Florida Division of Emergency Management
2555 Shumard Oak Boulevard
Tallahassee, Florida 32399-2100
850-413-9900
http://www.dca.state.fl.us/fdem/
http://floridadisaster.org/

Florida Insurance Council
Post Office Box 13686
Tallahassee, Florida 32317
850-386-6668
http://www.flains.org/

Institute for Business & Home Safety
1408 North Westshore Boulevard, Suite 208
Tampa, Florida 33607
1-800-657-4247
www.ibhs.org

Insurance Information Institute
110 Williams Street
New York, New York 10038
212-346-550
http://www.iii.org

National Fire Protection Association
1 Batterymarch Park
Quincy, Massachusetts 02169-7471
617-770-3000
http://www.nfpa.org/catalog/home/index.asp
http://nfpa.gcnpublishing.com/

Ocala-Marion County Economic Development Corporation
Post Office Box 459
Ocala, Florida 34478-0459
352-629-2757
www.ocalaedc.org

Tampa Bay Regional Planning Council
9455 Koger Boulevard, Suite 219
St. Petersburg, Florida 33702
727-570-5151

US Department of Agriculture
Farm Service Agency
1400 Independence Ave., S.W.
Washington, DC 20250-0506
Telephone: (202) 720-1632
http://www.fsa.usda.gov/

US Small Business Administration
409 Third Street, SW
Washington, D.C. 20416
202-205-6734
www.sba.gov

Web Sites

Institute for Business & Home Safety	www.ibhs.org
Federal Alliance for Safe Homes (FLASH)	www.flash.org
Florida Emergency Preparedness Association	www.fepa.org
Florida Small Business Development Center	http://www.floridasbdc.com/
Florida Insurance Council	http://www.flains.org/

Department of Homeland Security	www.dhs.gov/dhspublic/
Federal Emergency Management Agency	www.fema.gov
US Fire Administration	www.usfa.fema.gov
Small Business Administration	www.sba.gov
Florida Division of Emergency Management	http://www.floridasbdc.com/

American Red Cross	www.redcross.org
Salvation Army	www.salvationarmy.org

National Hurricane Center	www.nhc.noaa.gov
National Oceanic and Atmospheric Administration	www.noaa.gov
National Weather Service	www.nws.noaa.gov

Unit Ten
APPENDICES

Appendix **Page**

Vulnerability Analysis Chart

TYPE OF EMERGENCY	Probability	Human Impact	Property Impact	Business Impact	Internal Resources	External Resources	Total
	High 5 ◄►1 Low	High Impact 5 ◄► 1 Low Impact			Weak Resources 5 ◄► 1 Strong Resources		

The lower the score the better

Source: Federal Emergency Management Agency

Training, Drills and Exercises Chart

	January	February	March	April	May	June	July	August	September	October	November	December
MANAGEMENT ORIENTATION/REVIEW												
EMPLOYEE ORIENTATION/REVIEW												
CONTRACTOR ORIENTATION/REVIEW												
COMMUNITY/MEDIA ORIENTATION/REVIEW												
MANAGEMENT TABLETOP EXERCISE												
RESPONSE TEAM TABLETOP EXERCISE												
WALK-THROUGH DRILL												
FUNCTIONAL DRILLS												
EVACUATION DRILL												
FULL-SCALE EXERCISE												

Source: Federal Emergency Management Agency

Appendix 3

Open for Business Worksheet

Insurance Coverage Discussion Form

Use this form to discuss your insurance coverage with your agent. Having adequate coverage now will help you recover more rapidly from a catastrophe.

Insurance Agent: _____

Address: _____

Phone: _____ **Fax:** _____ **Email:** _____

INSURANCE POLICY INFORMATION

Type of Insurance	Policy No.	Deductibles	Policy Limits	Coverage (General Description)

Do you need Flood Insurance? Yes No

Do you need Earthquake Insurance? Yes No

Do you need Business Income and Extra Expense Insurance? Yes No

Other disaster-related insurance questions:

_____

_____

_____

_____

Source: Institute for Business & Home Safety

Appendix 4

Open for Business Worksheet
Creditor Contact Information

Use this form to keep a list of the major creditors you need to contact in the event of a disaster. Make additional copies as needed.

Keep one copy of this list in a secure place on your premises and another in an off-site location.

CREDITORS

Bank Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number: _____

Bank Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number: _____

Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number: _____

Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number: _____

Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number: _____

Company Name: _____

Street Address: _____

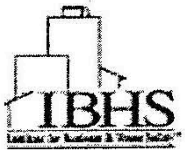
City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number: _____

Source: Institute for Business & Home Safety

Appendix 5



Open for Business Worksheet

Supplier Contact Information

Use this form to:

1. Keep a list of the major suppliers you need to contact in the event of a disaster, and
2. Know what their disaster plans are in the event that they experience a disaster.

Make additional copies as needed.

Keep one copy of this list in a secure place on your premises and another in an off-site location.

SUPPLIERS

1. 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:

1A. Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number: _____

2. 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:

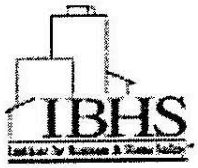
2A. Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number: _____



3. 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:

3A. Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number:_____

4. 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:

4A. Company Name: _____

Street Address: _____

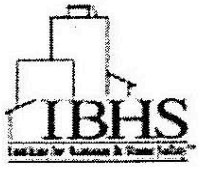
City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number:_____

Source: Institute for Business & Home Safety

Appendix 6



Open for Business Worksheet

Key Customer Information

Use this form to:

1. Keep a list of your key customers that you need to contact in the event of a disaster, and
2. Where these customers can obtain alternative resources until you reopen.

Make additional copies as needed.

Keep one copy of this list in a secure place on your premises and another in an off-site location.

CUSTOMERS

1. Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number: _____

If my company experiences a disaster, my customer will obtain supplies/materials from the following:

1A. Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number: _____

2. Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number: _____

If my company experiences a disaster, my customer will obtain supplies/materials from the following:

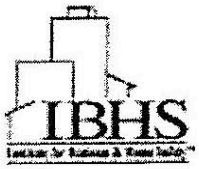
2A. Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number: _____



3. Company Name: _____

Street Address: _____

City _____ State_____ Zip Code _____

Phone:_____ Fax: _____ E-mail:_____

Contact Name: _____ Account Number: _____

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

3A. Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number:_____

4. Company Name: _____

Street Address: _____

City _____ State_____ Zip Code _____

Phone:_____ Fax: _____ E-mail:_____

Contact Name: _____ Account Number: _____

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

4A. Company Name: _____

Street Address: _____

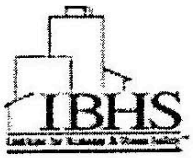
City _____ State _____ Zip Code _____

Phone: _____ Fax: _____ E-mail: _____

Contact Name: _____ Account Number:_____

Source: Institute for Business & Home Safety

Appendix 7



Open for Business Worksheet

Emergency Contact List

Keep this emergency contact list available for you and your employees in the event of an emergency. Attach a list of employee emergency contact numbers to this list.

Local Police Department: _____

Local Fire Department: _____

Ambulance Service: _____

Hospital: _____

Insurance Company: _____

Agent: _____

Policy Number: _____

Telephone Company: _____

Gas/Heat Company: _____

Electric Company: _____

Building Manager: _____

Building Security: _____

Local Small Business Administration Office: _____

Federal Emergency Management Agency Regional Office: _____

Local Newspaper: _____

_____

_____

Local Radio Stations: _____

_____

_____

_____

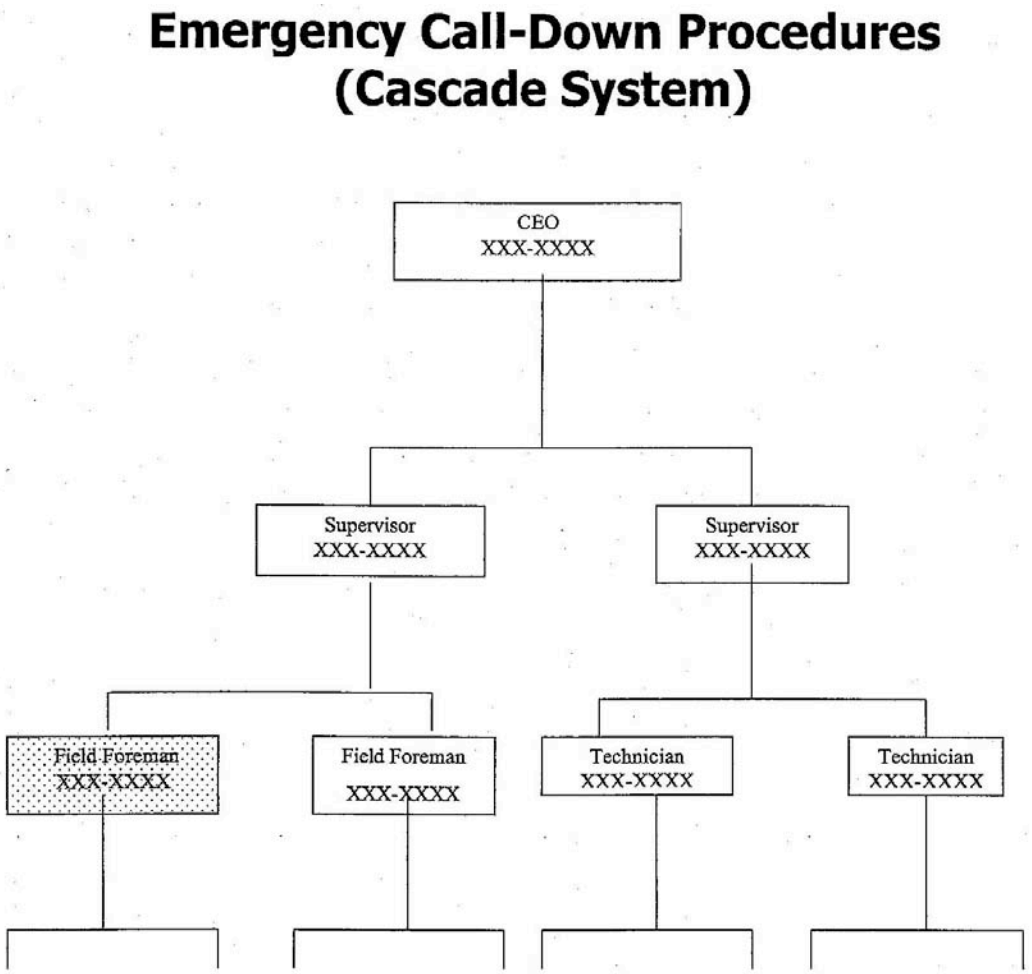
Local Televisions Stations: _____

_____

_____

Source: Institute for Business & Home Safety

Appendix 8



Source: Tampa Bay Regional Planning Council

Appendix 9

Facility Disaster Supplies Kit

One of the most important tools for emergency preparedness is the Disaster Supplies Kit. Below are the most important items for your kit at home. At the office, the amount of food and water should reflect what is necessary for a minimum of three days. Stock up today and store in a water-resistant container. Replenish as necessary, especially at the beginning of hurricane season June 1.

- ☐ Two weeks supply of prescription medicines
- ☐ Two weeks supply of non-perishable/special dietary foods
- ☐ Drinking Water/containers - 1 gal/per person/per day (minimum 3 days)
- ☐ Flashlights and batteries for each employee
- ☐ Portable radio and batteries
- ☐ First aid book and kit including bandages, antiseptic, tape, compresses, aspirin and aspirin pain reliever, anti-diarrhea medication, antacid, Syrup of Ipecac (used to promote vomiting if advised by the Poison Control Center)
- ☐ Mosquito repellant & citronella candles
- ☐ Fire extinguisher (small canister, ABC type)
- ☐ Instant tire sealer
- ☐ Whistle and/or distress flag
- ☐ Two coolers (one to keep food; one to go get ice)
- ☐ Plastic tarp, screening, tools and nails, etc.
- ☐ Water purification kit (tablets, chlorine (plain) and iodine)
- ☐ Infant necessities (medicine, sterile water, diapers, ready formula, bottles), if needed
- ☐ Clean-up supplies (mop, buckets, towels, disinfectant)
- ☐ Camera and film
- ☐ Non-electric can opener
- ☐ Extra batteries for camera, flashlights, radio, portable TV & lamps, etc.
- ☐ Garbage Can or bucket with tight-fitting lid (for emergency toilet)
- ☐ Plastic trash bags
- ☐ Toilet paper, paper towels and pre-moistened towelettes

If there is a chance employees would remain at the facility, also consider:

- ☐ Pillows, blankets, sleeping bags or air mattresses
- ☐ Extra clothing, shoes, eyeglasses, etc.
- ☐ Folding chairs, lawn chairs or cots
- ☐ Personal hygiene items (toothbrush, toothpaste, deodorant, etc.)
- ☐ Quiet games, books, playing cards, etc.

Precious commodities before and after a disaster

- ☐ Cash (With no power, banks may be closed, checks and credit cards unaccepted, and ATMs may not be operational).
- ☐ Charcoal, Wooden Matches and Grill
- ☐ Ice

Source: Tampa Bay Regional Planning Council

Appendix 10

The Evacuation "GO BOX"

The "Go Box" contains copies of important documents, equipment and supplies essential for the business to continue to operate. It should be stored in a fire-proof secure container in an alternate location. Below are recommended items; however, each business unit should discuss and specifically designate the contents of their "Go Box".

Recommended "Go Box" contents:

- ☐ Copy of emergency contact list of employees and key customers/clients
- ☐ Copy of insurance policies, agent contact information
- ☐ Copy of listing of emergency vendors (contractors, plumbers, electricians, restoration contractors, mold remediation, etc.)
- ☐ Copy of Listing of vendors & suppliers (and alternates) essential for mission critical activities
- ☐ Back up files/ tapes or server(s) of electronic data
- ☐ Copy of essential policies, emergency procedures, Business Continuity Plans
- ☐ General Office supplies plus any special forms, etc. used in your business
- ☐ Other _____
- ☐ Other _____
- ☐ Other _____
- ☐ Other _____
- ☐ Other _____
- ☐ Other _____

Documentation Requirements for a SBA disaster Loan:

- ☐ Corporations/ Partnerships: Copy of 3 years tax returns / 1 year personal tax returns on principles (affiliates with greater than 20% interest) / One year tax returns on affiliated business entity
- ☐ Sole Proprietorships: Copy of 3 years tax returns with Schedule C
- ☐ Copy of Current Profit & Loss Statement (within 90 days)
- ☐ Copy of Listing of aged accounts receivables/ payables
- ☐ Copy of Listing of inventory
- ☐ Copy of Schedule of Liability
- ☐ Copy of Balance sheet (as recent as possible)

Source: Tampa Bay Regional Planning Council

Appendix 11

Open for Business Worksheet
Computer Hardware Inventory

Use this form to:

- Log your computer hardware serial and model numbers. Attach a copy of your vendor documentation to this document.
- Record the name of the company from which you purchased or leased this equipment and the contact name to notify for your computer repairs.
- Record the name of the company that provides repair and support for your computer hardware.

Make additional copies as needed.

Keep one copy of this list in a secure place on your premises and another in an off-site location.

HARDWARE INVENTORY LIST

Hardware (CPU, Monitor, Printer, Keyboard, Mouse)	Hardware Size, RAM & CPU Capacity	Model Purchased	Serial Number	Date Purchased	Cost

COMPUTER HARDWARE INVENTORY (continued):

Hardware Vendor or Leasing Company Information

Company Name: _____

Street Address: _____

City _____ State_____ Zip Code _____

Phone:_____

Fax: _____

E-mail:_____

Contact Name: _____

Account Number: _____

Hardware Supplier/Repair Vendor Information

Company Name: _____

Street Address: _____

City _____ State_____ Zip Code _____

Phone:_____

Fax: _____

E-mail:_____

Contact Name: _____

Account Number: _____

Source: Institute for Business & Home Safety

Appendix 12

Open for Business Worksheet

Computer Software Inventory

Use this form to:

- Log your computer software serial and license numbers, and attach a copy of your licenses to this document.
- Record the name of the company from which you purchased or leased this software from, and the contact name to notify for your software support.
- Record the name of the company where you store backups of your computer information, including the contact name and how often backups are sent to this location.

Make additional copies as needed.

Keep one copy of this list in a secure place on your premises and another in an off-site location.

SOFTWARE INVENTORY LIST

Software Title and Version	Serial/Product ID Number	No. of Licenses/ License Number	Date Purchased	Cost

COMPUTER SOFTWARE INVENTORY (continued):

Software Vendor or Leasing Company Information

Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____

Fax: _____

E-mail: _____

Contact Name: _____

Account Number: _____

Off-Site Data Backup Information

Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____

Fax: _____

E-mail: _____

Contact Name: _____

Account Number: _____

Source: Institute for Business & Home Safety

Appendix 13

Open for Business Worksheet

Computer Peripheral Inventory

Use this form to:

- Log your computer peripherals' (modems, zip drives, scanners, etc.) serial and license numbers. Attach a copy of your vendor documentation to this document.
- Record the name of the company you purchased or leased this equipment and the contact name to notify for your computer repairs.
- Record the name of the company that provides repair and support for your computer peripherals.

Make additional copies as needed.

Keep one copy of this list in a secure place on your premises and another in an off-site location.

PERIPHERAL INVENTORY LIST

Hardware (CPU, Monitor, Modem, Zip Drives, etc.)	Disk Capacity, RAM	Model Purchased	Serial/Product Number	Date Purchased	Cost

COMPUTER PERIPHERAL INVENTORY (continued):

Peripheral Vendor or Leasing Company Information

Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____

Fax: _____

E-mail: _____

Contact Name: _____

Account Number: _____

Peripheral Support Vendor Information

Company Name: _____

Street Address: _____

City _____ State _____ Zip Code _____

Phone: _____

Fax: _____

E-mail: _____

Contact Name: _____

Account Number: _____

Source: Institute for Business & Home Safety

Appendix 14

Cyber Security Threat Assessment

SECURITY CHECKLIST	Yes	No
PHYSICAL SECURITY		
1. Is your computing area and equipment physically secured?		
2. Are there procedures in place to prevent terminals from being left in an logged-on state, however briefly?		
3. Are screens automatically locked after 10 minutes idle?		
4. Are modems set to Auto-Answer OFF (not to accept incoming calls)?		
5. Are your PCs inaccessible to unauthorized users (e.g., located away from public areas)?		
6. Does your staff wear ID badges?		
7. Do you check the credentials of external contractors?		
8. Do you have procedures for protecting data during equipment repairs?		
9. Is waste paper binned or shredded?		
10. Do you have procedures for disposing of waste material?		
11. Do your policies for disposing of old computer equipment protect against loss of data (e.g., by reading old disks and hard drives)?		
12. Do you have policies covering laptop security (e.g., cable lock or secure storage)?		
ACCOUNT AND PASSWORD MANAGEMENT		
13. Do you ensure that only authorized personnel have access to your computers?		
14. Do you require and enforce appropriate passwords?		
15. Are your passwords secure (not easy to guess, regularly changed, no use of temporary or default passwords)?		
16. Are your computers set up so that staff entering passwords cannot be viewed by others?		
CONFIDENTIALITY OF SENSITIVE DATA		
17. Are you exercising responsibility to protective sensitive data under our control?		
18. Is your most valuable or sensitive data encrypted?		
DISASTER RECOVERY		
19. Do you have a current business continuity plan?		
SECURITY AWARENESS AND EDUCATION		
20. Are you providing information about computer security to your staff?		
21. Are employees taught to be alert to poss ible security breaches?		

Source: Tampa Bay Regional Planning Council

Appendix 15

Cyber Security Checklist

This is an example of a threat checklist using 0-5 rating scales for impact and likelihood.

IMPACT SCALE	LIKELIHOOD SCALE
0 Impact is negligible	0 Unlikely to occur
1 Effect is minor; major agency operations are not affected.	1 Likely to occur less than once per year
2 Agency operations are unavailable for a certain amount of time, costs are incurred, public/customer confidence is minimally affected.	2 Likely to occur once per year
3 Significant loss of operations; significant impact on public/customer confidence.	3 Likely to occur once per month
4 Effect is disastrous; systems are down for an extended period of time; systems need to be rebuilt and data replaced.	4 Likely to occur once per week
5 Effect is catastrophic; critical systems are offline for an extended period; data are lost irreparably corrupted; public health and safety are affected.	5 Likely to occur daily

Threats	Impact (0-5)	Likelihood (0-5)	Total (Impact x Likelihood)
GENERAL THREATS			
Human error: 1. Accidental destruction, modification, disclosure, or incorrect classification of information. 2. Ignorance: Inadequate security awareness, lack of security guidelines, lack of proper documentation, lack of knowledge. 3. Workload: Too many or too few system administrators; highly pressured users. 4. Users may inadvertently give information on security weaknesses to attackers. 5. Incorrect system configuration. 6. Security policy not adequate. 7. Security policy not enforced. Security analysis may have omitted something important, or be wrong.			

Threats	Impact (0-5)	Likelihood (0-5)	Total (Impact x Likelihood)
1. Dishonesty: Fraud, theft, embezzlement, selling of confidential agency information.			
2. Attacks by "social engineering": • Attackers may use telephone to impersonate employees to persuade users/administrators to give username/passwords/modem numbers, etc. • Attackers may persuade users to execute Trojan horse programs.			
3. Abuse of privileges/trust			
4. Unauthorized use of "open" terminals/PCs.			
5. Mixing of test and production data or environments			
6. Introduction of unauthorized software or hardware.			
7. Time bombs: Software programmed to damage a system on a certain date.			
8. Operating system design errors: Certain systems were not designed to be highly secure.			
9. Protocol design errors: Certain protocols were not designed to be highly secure. Protocol weaknesses in TCP/IP can result in: • Source routing, DNS spoofing, TCP sequence guessing, unauthorized access. • Hijacked sessions and authentication session/transaction replay; data is changed or copied during transmission. • Denial of service, due to ICMP bombing, TCP_SYN flooding, large PING packets, etc.			
10. Logic bomb: Software programmed to damage a system under certain conditions.			
11. Viruses in programs, documents, e-mail attachments.			
IDENTIFICATION/AUTHORIZATION THREATS			
1. Attack programs masquerading as normal programs (Trojan horses).			
2. Attack hardware masquerading as normal commercial hardware.			
3. External attackers masquerading as valid users or customers.			

Threats	Impact (0-5)	Likelihood (0-5)	Total (Impact x Likelihood)
4. Internal attackers masquerading as valid users or customers.			
5. Attackers masquerading as helpdesk/support personnel.			
RELIABILITY OF SERVICE THREATS			
1. Major natural disasters: fire, smoke, water, earthquake, storms/hurricanes/tornadoes, power cuts, etc.			
2. Minor natural disasters, of short duration, or causing little damage.			
3. Major human-caused disasters: war, terrorist incidents, bombs, civil disturbance, dangerous chemicals, radiological accidents, etc.			
4. Equipment failure from defective hardware, cabling, or communications system.			
5. Equipment failure from airborne dust, electromagnetic interference, or static electricity.			
6. Denial of service: • Network abuse: Misuse of routing protocols to confuse and mislead systems. • Server overloading (processes, swap space, memory, "tmp" directories, overloading services). • E-mail bombing. • Downloading or receipt of malicious Applets, ActiveX controls, macros, Postcript files, etc.			
7. Sabotage: Malicious, deliberate damage of information or information processing functions. • Physical destruction of network interface devices, cables. • Physical destruction of computing devices or media. • Destruction of electronic devices and media by electromagnetic radiation weapons (HERF Gun, EMP/T Gun). • Theft. • Deliberate electrical overloads or shutting off electrical power. • Viruses and/or worms. Deletion of critical system files.			
PRIVACY THREATS			

Threats	Impact (0-5)	Likelihood (0-5)	Total (Impact x Likelihood)
1. Eavesdropping: • Electromagnetic eavesdropping/Van Eck radiation. • Telephone/fax eavesdropping (via "clip-on," telephone bugs, inductive sensors, or hacking the public telephone exchanges. • Network eavesdropping: Unauthorized monitoring of sensitive data crossing the internal network, unknown to the data owner. • Network eavesdropping: Unauthorized monitoring of sensitive data crossing the Internet, unknown to the data owner. • Subversion of DNS to redirect e-mail or other traffic. • Subversion of routing protocols to redirect e-mail or other traffic. • Radio signal eavesdropping. Rubbish eavesdropping (analyzing waste for confidential documents, etc.).			
INTEGRITY/ACCURACY THREATS			
1. Malicious, deliberate damage of information or information processing functions from external sources.			
2. Malicious, deliberate damage of information or information processing functions from internal sources.			
3. Deliberate modification of information.			
ACCESS CONTROL THREATS			
1. Password cracking (access to password files, use of bad (blank, default, rarely changed) passwords).			
2. External access to password files, and sniffing of the network.			
3. Attack programs allowing external access to systems (back doors visible to external networks).			
4. Attack programs allowing internal access to systems (back doors visible to internal networks).			
5. Unsecured maintenance modes, developer backdoors			
6. Modems easily connected, allowing uncontrollable extension of the internal network.			

Threats	Impact (0-5)	Likelihood (0-5)	Total (Impact x Likelihood)
7. Bugs in network software which can open unknown/ unexpected security holes. (Holes can be exploited from external networks to gain access. This threat grows as software becomes increasingly complex.)			
8. Unauthorized physical access to system.			
REPUDIATION THREATS			
1. Receivers of confidential information may refuse to acknowledge receipt.			
2. Senders of confidential information may refuse to acknowledge source.			
LEGAL THREATS			
1. Failure to comply with regulatory or legal requirements (e.g., to protect confidentiality of employee data).			
2. Liability for acts of internal users or attackers who abuse the system to perpetrate unlawful acts (e.g., incitement to racism, gambling, money laundering, distribution of pornographic or violent material).			
3. Liability for damages if an internal user attacks other sites.			

Source: Tampa Bay Regional Planning Council

Appendix 16

Vital Information Management

The vital information that allows the office to function must have "back-ups" off-site and is divided into sections:

- **Financial**
  - Copy of all bank account numbers and their balances
  - Copy of all CD account numbers and balances
  - Accounts Receivable information
  - Employee insurance information
  - Business insurance information
    - All leased and company vehicles
    - All equipment insurance
      - Extended warranties and/or policies
  - 401-K Information
  - Business account information
    - Account numbers & company contact telephone numbers
      - Telephone
      - Electric (any utility your office receives service from)
      - Company credit cards
      - All customers
      - All vendors

- **Contractual**
  - Copy of any contracts between your company and another entity
  - Copy of building lease
  - Copy of any equipment leases
    - All leased and company vehicles
    - Copier
    - Postage machine
    - Telephones or other leased items
  - Copy of City, County & any State business licenses
  - Copy of original charter
  - Copy of company By-laws
  - Copy of Employee Handbook
  - Copy of any current company Strategic or Business Plan

- **Inventory Lists**
  - Furniture
  - Equipment
    - Calculators
    - Cameras
    - TVs
    - Video screen

- Binders
- Usable materials
  - Brochures
  - Any materials purchased in large amounts
- List of personal items from each employee's office

- **Computer Equipment (include serial numbers)**
  - Monitors
  - Keyboards
  - Towers
  - Lap top computer
  - Scanner/Copier
  - Printers

- **For Medically Related Businesses**
- In addition to items listed in this outline, all necessary patient information (pertinent history, etc.)
- All pertinent information related to medical equipment
- Copies of all medical degrees earned by doctors and staff

- **Membership Information**
- **This section is mostly used in "not for" and "non" profit organizations**
  - Copy of current membership list
    - Include all pertinent information including email address
  - Copy of membership dues
    - When paid, how much, any outstanding amounts, etc…
  - Copies of the most recent year's information
    - Progress reports, Guides, most recent brochures and printed materials.
    - Most recent Quarterly Report information
    - Copy of minutes from last four to six Board Meetings
      - For history & continuity
    - Minutes from any critical committees the company either hosts or attends

Community & Business Contacts

- Copy of names & telephone numbers of contacts from:
  - Utility companies
  - Telephone
  - City government
  - County government
  - Fire Department
  - Police & Sheriff Departments
  - Hospitals
  - Current company projects

- Most items should be copied to disk or CDROM. There will be many documents not found in the computer system and standard "hard" copies should be made of them. Scanned documents are easier to store. It is also worth consideration to keep the "originals" in the bank deposit drawer and work from a copy of the document.

- ***LOCATIONS FOR COMPANY INFORMATION SAFE-KEEPING:***

  - Each staff member will keep a set of diskettes at their residence that pertains to their section of the business.

  - The owner or President/CEO will be the only person to have an entire set of disks, which will also be kept at his/her residence.

  - One set of the disks will be sealed in an envelope and sent to an entity that the head of the company deems trustworthy, **in another state**, (reasoning for this is in case of a disaster potentially affecting the entire state).
    - Should there be a state disaster, the disks kept "out-of-state" could end up being the only intact set to operate the business from.
    - The set sent out of state will be updated annually or semi-annually, whichever is deemed most efficient.
      - The out-of-state entity holding this set will merely Fed Ex them to business at a pre-designated time, to be updated and returned back to them.
- The disks each staff member is responsible for will be updated quarterly, or as necessary.

- "Paper" copies of documents should be kept in **two** places
- A fireproof safe (preferably with minimum 4 hour protection) on site
    - A safe deposit drawer in a local banking institution

- A separate computer tower, screen, keyboard and mouse could possibly be placed at another designated site, for use by the company if the office was rendered un-usable. The second (and probably best) option would be to keep "laptop" at the residence of the owner, CEO, President or Office Manager for such emergencies. This enables your business to be up and running immediately, with reduced interruption given the circumstances.

Source: Ocala/Marion County Economic Development Council

Appendix 17

Protection of Data – Backups, Software and Policies

Backups: Creating a mirror image of the intangible data onto tangible media (disk, tape, CD, etc.) provides a backup of this information. When the original data is rendered useless the backups can then be used to re-create the data. When client-host and distributive processing becomes more popular it is important to backup all workstations since they all work in a synergistic whole.

System: System backups provide a spare copy of all the information on a computer system. The operating system (Windows, NT, etc.), application software, and volatile data are all backed-up. This should be done on individual workstations as well as on host servers.

Monthly: Even if no major hardware or software changes are made, system backups should be done on a monthly basis. Some software products can dynamically make changes to pointer files and other indexes that pertain to user data, but are actually stored elsewhere on the system.

Hardware or Software Changes: When hardware changes are made they are often saved in the CMOS. Battery failure could cause the CMOS to "forget" the hardware configuration making restoration from system backups necessary. A system backup should be done just prior to any major hardware or software changes. Another separate system backup should be done just after the changes. This provides a way to return to "square one" should any problems occur.

Operating System backup of Backup Software: Some operating systems provide basic programs for making backups. However, most systems use more efficient software in addition to the basic operating system to make backups. Before restores can be done to recover information from backups the software used to make the backups to begin with needs to be put back on the computer. By using the operating system to backup the software used to make the bulk of the backups it insures that the more efficient software can be restored using the basic operating system. Once the backup software is restored it can then be used to restore the rest of the system.

Create Bootable Disk of Operating System (Windows, NT, etc.) After a damaged computer has been repaired or replaced the operating system needs to be restored. For this restoration to take place the computer needs to be powered-up or "booted" using the operating system (OS), This typically means that a disk or CD replicating the original OS needs to be used. Some Local Area Networks (LAN's) using a Network Operating System (NOS) use a Network Operating System that can be restored using disks, CD's or tapes created from more elaborate backup software packages.

Data Only: Unlike system software, which typically doesn't change often, user data changes daily. Making backup of data is like having tangible insurance in that the hours of work a computer user has done has been protected.

Daily: System backups usually only need to be done on a monthly, or at most weekly, basis. However, most non-home PC's should have their data backed up daily.

Monday – Friday: Each day of the workweek should have its own data set backup. In other words if the workweek is Monday through Friday and it takes two tapes each day to do a data backup then a total of ten tapes should be used on a rotational basis.

Weekly: In addition to the daily backup sets a separate data backup set should be done weekly. This backup is then archived in case past information needs to be retrieved.

Fridays: Weekly data backups should be kept for a period of five weeks. This assures that past information can be retrieved on a week-by-week basis for up to a month's period back.

Monthly: Separate data backup sets should also be done on a monthly basis. These backups should be kept even after data is purged from the system for later referral. Data is typically not purged for at least one year.

Archives: Monthly data backup sets should be kept until archival backups are made. Archival backups are typically made yearly and/or just prior to purging obsolete data from the computer. This insures an audit trail is maintained in case the information needs to be retrieved after it is purged.

Storage: Correct storage of backups is a necessity. Backups that have been damaged by incorrect storage may not restore.

On-site: One set of systems backups and data backups should be kept on-site at the location of the computer systems. The latest backups are usually the ones kept on-site.

Paper Fire Safes: Fire safes for protecting papers reduce the flash point of documents. This is accomplished by a cement-like material in the walls of the safe that evaporates a vapor into the safe to dampen the paper. This allows the temperature to rise to the 300 – 400+ degree range without igniting the paper. Important papers to be stored should also include software license numbers since they are often required if a software product is to be reinstalled.

Magnetic Media Fire Safes: Fire safes for tapes, disks and CD's differ from fire safes designed to protect paper. Condensing moisture can damage magnetic media, so these safes typically do not contain vapor-inducing materials. Tapes, disks, CD's and other media should be kept in safes that insulate against fire heat to keep internal temperatures below 125 degrees. Safes should not be opened for at least 24 hours after fire exposure to allow the internal temperature to stabilize gradually. It is important to keep the original installation disks and CD's for software packages should the need arise to reinstall a given program.

Off-site: At least two system and data backup sets should be kept off-site from the location of the computer systems. If a large-scale disaster occurs at the computer system location the on-site backups may be destroyed. The geographic distance needed for off-site locations depends on the anticipated threats; across town is sufficient for a building fire, for hurricanes

the distance should be 30+ miles, for earthquakes it may require locating in a different area of the country.

Paper Fire Vaults: The storage space needed for paper documents can expand quickly depending on the amount of paper generated by a system. Critical papers can be kept in fire safes, but large volumes of paper may require a vault. Fire vaults are entire rooms that are protected against fire rather than individual safes.

Magnetic Media Fire Vaults: Vaults for magnetic media are also entire rooms protected against fire rather than having to go to the expense of many individual fire safes. Magnetic media fire vaults differ from paper fire vaults in that the internal temperatures should be kept lower and fire suppression systems are usually Halon or Inergen instead of water sprinklers.

Magnetic Media: Ironically, as organizations transfer documents to magnetic media, they may actually be shortening the storage life of the information. Properly stored paper can last for decades or even centuries. However, disks have a shelf life of one to two years, tapes/drives three to five years and CD's ten plus years. For irreplaceable information it is best to have paper documents to augment the magnetic media. One example is the popularity of video wills; paper wills should still be done in the event the magnetic VHS tape is no longer readable.

Restores: Backup data sets are only of use if they can be restored properly. Financial institutions are often required to test their backups and disaster recovery procedures two times a year. Some LAN server backup products make "images" of volumes instead of using a file-by-file method; this drastically reduces the number of steps needed to recover a system.

Boot With Copy of Operating System: Computer systems need to be started with an operating system (OS) in order to function. A copy of the OS (Windows, NT, etc.) should be kept with each backup set. Other operations, such as drive partitioning, may also have to be performed prior to restoring backup data sets.

Restore Backup Software: Before a backup set can be restored the software that was used to create the backups originally must be placed back onto the computer system. Backups are usually unreadable by the native operating system and can only be read by the dedicated backup software.

Restore System Backup: After the backup software itself is loaded onto the computer system the system backup data can be restored. Once the system backups are restored the computer should then indeed be back in an operable mode.

Restore Latest Data: Although a computer system may be once again operational after restoring system backups, the data may not be current. If data-only backups were made subsequent to the system backup then they too should be restored in order to bring the information up to the most current possible state.

Hot-site: Disasters that destroy data and software can also destroy the computer hardware that runs the software. A hot-site is an alternate location that has compatible hardware and facilities available to restore software. "Cold-sites" cost less, but don't have the equipment already installed in the facility.

- Location: The location of a potential hot-site should be considered. In a hurricane or earthquake, for instance, the disaster area could be tens of miles wide. If widespread disasters are identified in a risk assessment the hot-site location should be distant enough to be unaffected by the same disaster.
- Equipment: The computer hardware and other equipment should be compatible with the original system. Other office equipment such as phone systems, fax machines, and employee workspaces should also be examined.
- How soon to utilize: One key decision to be made, particularly during a "predictable" disaster such as a hurricane, is to decide how soon to use a hot-site.
- Too-soon operating costs: It might be thought that it is never too soon to utilize a hot-site if a potential disaster, such as a hurricane, is approaching. However, there are costs involved in moving backups, equipment and personnel to a hot-site. If the disaster doesn't occur then the costs were unnecessarily incurred.
- Too-late alternate site: In an effort to save unnecessary costs the decision could be made to wait on the declaration of a disaster. However, hot-sites generally have multiple contracts with other clients that may also be declaring disasters. For this reason it is advisable to have an alternate ho-site identified in he event that the primary site is already occupied.

Internet Backup: Many companies are investigating the virtues of online data backup, a process that involves transferring backups over the Internet and storing them in secure, offsite vaults. The system mitigates the amount of work that must be done in order to transfer data to a secure location and insures that is well protected. The system provided easy access and quick retrieval, often within minutes.

Source: Tampa Bay Regional Planning Council per Strategic Research Corporation

Appendix 18

Emergency Evacuation Procedures

Evacuations are more common than many people realize. Hundreds of times each year, transportation and industrial accidents release harmful substances, forcing thousands of people to leave their homes. Fires and floods cause evacuations even more frequently. And almost every year, people along the Gulf and Atlantic coasts evacuate in the face of approaching hurricanes. When community evacuations become necessary, local officials provide information to the public through the media. In some circumstances other warning methods, such as sirens or telephone calls, are also used.

The amount of time you have to evacuate will depend on the disaster. If the event can be monitored, like a hurricane, you might have a day or two to get ready *(See what to do before, during and after a Hurricane*). However, many disasters allow no time for people to gather even the most basic necessities.

Planning for evacuation

Ask your local emergency management agency about community evacuation plans. Learn evacuation levels and routes. In your planning, consider different scales of evacuations. In a hurricane, for example, thousands of coastal residents would evacuate, while much smaller area would be affected by a chemical release.

- ☐ Talk with your employees about the possibility of evacuation. Plan where you would go if you had to leave the building or the community. Ensure all employees would have transportation in the event of an emergency evacuation.

- ☐ Plan a place to meet your key employees in case you are separated from one another in a disaster. Designate someone to be the "checkpoint" so that employees can call that person to say they are safe.

- ☐ Assemble a disaster supplies kit for each facility. Include a battery-powered radio, flashlight, extra batteries, food, water and first aid kit. See the "*Disaster Supplies Kit*" for a complete list.

- ☐ Keep fuel in your car(s) if an evacuation seems likely. Gas stations may be closed during emergencies and unable to pump gas during power outages.

- ☐ Know how to shut off your facility's electricity, gas and water supplies at main switches and valves. Have the tools you would need to do this (usually adjustable pipe and crescent wrenches).

- ☐ Listen to a NOAA Weather Alert or battery-powered radio and follow local instructions.

Source: Tampa Bay Regional Planning Council

Shelter In Place Procedures

Stay inside the facility. This action will be recommended if there is a short release, a small amount of hazardous material in the air, or if time does not permit evacuation before the arrival of a cloud of toxic vapor. Take these steps to protect yourself and employees:

- ☐ Stay inside until local officials say you can leave safely. This will most likely be for no more than a few hours.
- ☐ **If your business has animals, if possible bring them indoors!**
- ☐ Close all doors and windows.
- ☐ Seal all gaps under doorways and windows with damp towels and duct tape.
- ☐ Turn off heating, cooling or ventilation systems.
- ☐ Listen to your local radio or TV stations for further instructions.
- ☐ Resist the impulse to go outdoors and "check things out" before given the "All Clear" by authorities.
- ☐ If you are told to protect your breathing, cover your nose and mouth with a damp handkerchief or other cloth folded over several times.

Source: Tampa Bay Regional Planning Council

Appendix 20

Employee Family Disaster Plan

EMPLOYEE FORM #
OUR FAMILY DISASTER PLAN

We don't like to think about a disaster in our community - much less take the time (and expense) to prepare our homes, families and business to weather a storm or other disaster. Yet, if you are armed with knowledge and a little forethought, you can save yourself and your family from potential injury and financial loss. It will also be critical that, as your employer, we know what your needs are before the event and ensure we can contact you after a disaster. To get started, first read the disaster preparedness guide provided to you. Then, prepare your own Family Disaster Plan by completing the checklist below:

1. KNOW YOUR RISK.
Will your family have to evacuate in a hurricane? (Y or N) _____
If yes, what Evacuation Level _____
100-year Flood Zone (Y or N)_____
If yes, if your home elevated above Base Flood Elevation? (Y or N) _____
Mobile home (Y or N)_____

2. HAVE AN EVACUATION PLAN.
If I do not have to evacuate, I will secure my house and stay. My employer can reach me at:
Phone _____
Emergency Phone No._____

If told to evacuate, we will go to:
Friends/Name_____
Phone No. _____
Emergency Phone No. _____

Hotel/Motel _____
Shelter_____
Out of the Area (Y or N) _____
Evacuation Route_____

3. Members of Your Family

1. First name_____
Last name _____
Age_____
Mobile phone_____
SS # _____
Employed by_____
Work phone _____
Blood type _____
Allergies_____
Special needs_____
_____

2. First name_____
Last name _____
Age_____
Mobile phone_____
SS # _____
Employed by_____
Work phone _____
Blood type _____
Allergies_____
Special needs_____
_____

3. First name_____
Last name _____
Age_____
Mobile phone_____
SS # _____
Employed by_____
Work phone _____
Blood type _____
Allergies_____
Special needs_____
_____

4. First name_____
Last name _____
Age_____
Mobile phone_____
SS # _____
Employed by_____
Work phone _____
Blood type _____
Allergies_____
Special needs_____
_____

3. PUT TOGETHER YOUR DISASTER SUPPLIES KIT (see list attached)

4. RELATIVES/FRIENDS TO CONTACT W/EMERGENCY INFO

Name/phone _____
_____
Name/phone_____
_____

5. MEDICAL AND INSURANCE. Call your agent. Make sure you are adequately covered. Put your Agent's Name/Phone Number and policy in a safe place along with an inventory of your belongings (a video tape is excellent).

Physician
Name _____
Address _____
Phone _____

Physician
Name _____
Address _____
Phone _____

Dentist
Name _____
Address _____
Phone _____

Medical Insurance
Carrier _____
Policy number _____
Address _____
Phone _____

Car Insurance
Carrier _____
Policy number _____
Address _____
Phone _____

Home Insurance
Carrier _____
Policy number _____
Address _____
Phone _____

6. INSPECT & SECURE YOUR HOME BEFORE THE STORM

- **Garage Doors** - 80% of the severe winds enter through an older, un-reinforced garage door. You can reinforce older metal doors (not wood) with kits sold at a home improvement store or replace with a hurricane-resistant one.
- **Entry Doors** - Double-bolt (top and bottom) all doors (Exterior doors should be solid wood or steel)
- **Gable Ends/ Roof** - During Hurricane Andrew, winds destroyed roofs due to un-reinforced gable ends. If your home was built before 1994, the gables should be retrofitted to strengthen the roof system. When you replace your roof, make sure the new sheathing is attached properly as well as new shingles or tiles.
- **Window Protection**- is very important to keep the winds out of your home. Once inside, internal wind pressure can lift your roof right off and expose you and your family to the winds. Windows should also be covered to reduce the risk of flying glass. Code approved shutters, impact resistant windows, plywood sheets (3/4"), shutter or other wind abatement systems should be considered.
- **Maintenance** is an important part of reducing the potential risk to damage. Keep your home in good repair.

7. FAMILY RESPONSIBILITIES

Make a list of tasks and who is responsible for each task: Don't forget to include the kids.

8. PLAN FOR PETS

Name _____
Tag number _____
Type of animal _____

Pet Shelter
Name _____
Address _____
_____
Phone _____

Name _____
Tag number _____
Type of animal _____

Veterinarian
Name _____
Address _____
Phone _____

9. DO YOU OR A LOVED ONE REQUIRE EVACUATION ASSISTANCE DUE TO SPECIAL NEEDS? CONTACT YOUR LOCAL EMERGENCY MANAGEMENT DEPARTMENT TO REGISTER TODAY.

Eldercare
Name _____
Address _____
Phone _____
Special Needs Shelter _____

Medications (Must be labeled with name and dosage. Including over-the-counter and samples.)
Living Will
Medical Bracelet-Allergies and Conditions
Copy of insurance card (s)
Emergency Contact Information
Special Diet Needs

Source: Tampa Bay Regional Planning Council

Appendix 21

What to do Before, During and After a Hurricane

- ☐ **Know Your Risk.** Check your hurricane evacuation level and FEMA flood maps to determine if your business location is vulnerable to storm surge or freshwater flooding. Have your building(s) inspected by a licensed professional to find out if your workplace is vulnerable to hurricane force winds and what is recommended to retrofit.

- ☐ **Take the Necessary Precautions.** If a storm threatens, secure your building. Cover windows. Cover and move equipment/furniture to a secured area.

- ☐ **ALWAYS Protect your data with backup files.** If dependent on data processing, consider an alternate site. Make provisions for alternate communications and power.

- ☐ **Make plans to work with limited cash, and no water, sewer or power for two weeks**. Store emergency supplies at the office.

- ☐ **Protect Your Employees.** Employee safety comes first! Prepare, distribute and exercise your business hurricane plan for recovery. Consider providing shelter to employees and their families and helping employees with supplies after the storm. Establish a rendezvous point and time for employees in case damage is severe and communications are disrupted. Establish a call-down procedure for warning and post-storm communications. Provide Photo IDs and a letter of authorization to enter the building.

- ☐ **Contact Your Customers & Suppliers** and share your communications and recovery plan in advance. Prepare a list of vendors to provide disaster recovery services.

- ☐ **Review Your Insurance Coverage.** Have your business appraised at least every five years. Inventory, document and photograph equipment, supplies and workplace. Have copies of insurance policies and customer service/home numbers. Obtain Business Interruption Insurance. Consider Accounts Receivable and Valuable Papers Coverage and Income Destruction Insurance. If you have Business Owners Protection Package (BOPP), check co-insurance provisions. **Remember: Flood damage requires separate coverage and is NOT covered under other insurance programs.**

- ☐ **After the Storm**. Use caution before entering your business. Check for power lines, gas leaks and structural damage. If any electrical equipment is wet, contact an electrician. Prepare loss information for insurance claims and get independent estimates of damages. Take pictures before cleanup. Minimize additional damage.

HURRICANE SEASON CHECKLIST
TAKE ACTION NOW

The hurricane season is **June** through **November**. **Be prepared!**

- ☐ Refer to the County Hurricane Evacuation Map. Locate your business facility or facilities and its evacuation level (color). Determine if and when you would have to evacuate your business from storm surge. REMEMBER: All work trailers and most warehouse/ storage facilities are extremely vulnerable to hurricane-force winds, regardless of location.

- ☐ If ordered to evacuate, DECIDE NOW how and when you will communicate with employees and where you can establish an alternative work site if your facility is severely damaged or inaccessible.

- ☐ Check your Disaster Supplies Kit and obtain any items you need for the office. Purchase a battery-powered National Weather Service weather alert radio.

- ☐ Keep your facility in good repair. Make sure loose roofing and siding is tacked down and dead or broken branches from trees are trimmed. Trees should be trimmed up off the ground and away from roofs to reduce the risk of fire as well.

- ☐ Survey your facility to determine if there are any improvements you can make to make the facility safer. You may contact the Small Business Development Center for an Energy/ Mitigation Audit that will identify cost-beneficial improvements for your facility. Or contact a professional engineer or licensed contractor to inspect your home for structural integrity.

- ☐ Make plans and purchase materials to protect your facility before the storm (plywood panels, steel, aluminum or plastic shutters; plastic sheeting, nails, etc.). Make sure all products meet the Dade County large missile impact test.

- ☐ Inventory your property (a video tape is excellent). Store with insurance and title papers and back-up tapes in a fireproof safe and keep a copy in a (fire-proof safe) home located in a non-evacuation zone.

- ☐ Make sure your address (number) is clearly marked on your facility.

- ☐ Whether you rent or own your facility, review your insurance policies with your agent now.

HURRICANE CHECKLIST
AS THE STORM APPROACHES

- ☐ Listen for weather updates on local stations and on NOAA Weather Radio. Don't trust rumors, and stay tuned to the latest information.
- ☐ Check your Disaster Supplies Kit at work. Obtain any needed items. Contact employees and instruct them to do the same.
- ☐ Instruct employees to refill prescriptions and to maintain at least a two-week supply during hurricane season.
- ☐ Clear property or tie down any items that could become flying missiles in high winds, e.g. lawn furniture, potted plants, and trashcans.
- ☐ Protect the windows and glass doors! If you do not have impact resistant windows, install shutters or plywood to cover glass. Brace double entry and garage doors at the top and bottom.
- ☐ Fill fleet cars and equipment gas tanks and check oil, water and tires. Gas pumps don't operate without electricity.
- ☐ Secure your boat early. Drawbridges will be closed to boat traffic after an evacuation order is issued.
- ☐ Obtain sufficient cash for business operations recognizing that banks and ATMs won't be in operation without electricity and few stores will be able to accept credit cards or personal checks.
- ☐ Run through BCP to ensure communications plan is up-to-date and employees are aware of responsibilities after the storm.
- ☐ Back up all computer data and ensure that back up is stored in a safe place off-site.
- ☐ Close the office in sufficient time to allow employees to secure their homes, obtain needed supplies and evacuate if necessary.

HURRICANE CHECKLIST
NO EVACUATION

If your facility is outside the evacuation area and NOT a work trailer, etc. your facility may be able to remain open or serve as shelter for employees.

☐ Make sure the windows and doors are protected and facility is secured.

☐ Clean containers for drinking water and sinks for storing cleaning water. Plan on three gallons per person, per day for all uses.

☐ Offering your facility as shelter to employees and their families who live in vulnerable areas or mobile homes will have benefits to your operations but may also have some liability. Check first with legal representation.

☐ Check the Disaster Supplies Kit. Make sure you have at least a two-week supply of non-perishable foods. Don't forget a non-electric can opener. Instruct any employees to augment the supply with a kit of their own.

☐ During the storm, everyone should stay inside and away from windows, skylights and glass doors. Find a safe area in your facility (an interior, reinforced room, closet or bathroom on the lower floor if the storm becomes severe.

☐ Wait for official word that the danger is over. Don't be fooled by the storm's calm "eye".

☐ If flooding threatens your facility, electricity should be turned off at the main breaker.

☐ If your facility loses power, turn off major appliances, such as the air conditioner and water heater to reduce damage.

IF YOU MUST EVACUATE: SECURING YOUR FACILITY

Stay tuned to your local radio and television stations for emergency broadcasts. If ordered to evacuate, you must do so immediately.

☐ Ensure important documents, files, back up tapes, emergency contact information, etc. are taken to a safer location. See **"Go Box".**
☐ Let employees, customers and vendors know your continuity plans. Make sure your employees have a safe ride.
☐ Turn off electricity, water and gas.
☐ Lock windows and doors.

HURRICANE CHECKLIST
AFTER THE STORM

After a disaster, your business may be without power, water, food or any of the services we rely on. Immediate response may not be possible, so residents and businesses must be prepared to be self-reliant for several weeks.

RE-ENTRY

- ☐ Be Patient. Access to affected areas will be controlled. You won't be able to return to your facility until search and rescue operations are complete and safety hazards, such as downed trees and power lines, are cleared. It may take up to three days for emergency crews to reach your area. It may take 2-4 weeks before utilities are restored. On barrier islands, it could take much longer.
- ☐ Stay tuned to your local radio station for advice and instructions about emergency medical aid, food and other forms of assistance.
- ☐ Security operations will include checkpoints. It will be critical for you and your employees to have valid identification with your current local address as well as something to prove your employment and need to get back into the area. It is recommended that businesses contact the county emergency management agency and local jurisdiction to determine what specifically would be required.
- ☐ Avoid driving. Roads will have debris that will puncture your tires. Don't add to the congestion of relief workers, supply trucks, law enforcement, etc.

SAFETY CHECKLIST

- ☐ Avoid downed or dangling utility wires. Metal fences may have been "energized" by fallen wires. Be especially careful when cutting or clearing fallen trees. They may have power lines tangled in them.
- ☐ Beware of snakes, insects or animals driven to higher ground by floods.
- ☐ Enter your home with caution. Open windows and doors to ventilate and dry your facility.
- ☐ If there has been flooding, have an electrician inspect your office before turning on the breaker.
- ☐ Be careful with fire. Do not strike a match until you are sure there are no breaks in gas lines. Avoid candles. Use battery-operated flashlights and lanterns instead.
- ☐ Use your telephone only for emergencies to keep lines open for emergency communications.

- ☐ Fueled by gas, generators can run appliances and fans.
- ☐ Sizes range from 750 watts that will run a fan and a light up to 8,000 watts that will practically run a house (except for the air conditioner).
- ☐ If you have lost power, don't connect a portable generator to building wiring (this could injure or kill neighbors or electrical crews).
- ☐ Plug equipment, computers, etc., directly into the generator.
- ☐ Place generator outdoors or in a well-ventilated area. Don't forget to check the oil every time you add gas. Conserve fuel by alternative appliances. For example, refrigerators can be kept cool by supplying power eight hours a day. Refrigerators require 400-1,000 watts.

REPAIRS

- ☐ Make temporary repairs to correct safety hazards and minimize further damage. This may include covering holes in the roof, walls or windows and debris removal.
- ☐ PROTECT YOURSELF FROM CONTRACTOR FRAUD! Only hire licensed contractors to do repairs. Check with the local Building Department to ensure the contractor is licensed. If you hire a contractor, don't pull the permits for them. If the contractor makes this request, it may be an indication that he is not properly licensed.
- ☐ Take photographs of all damage before repairs and keep receipts for insurance purposes.
- ☐ After assessing damage to your facility, contact your local building department for information on required building permits. Permits are always required for any kind of demolition or permanent repairs, reconstruction, roofing, filling and other types of site development. Report illegal flood plain development to your local building department.
- ☐ Local ordinances do not permit dumping in drainage canals or ditches because it causes backups and overflow in the system. Report illegal dumping.

WATER PRECAUTIONS

Whenever widespread flooding occurs, there is a potential for bacterial contamination. Bacteria, such as shigella and salmonella, can lead to life threatening dehydration for people if untreated by antibiotics. Disinfect any tap water you drink or use for cooking or cleaning. You must purify the tap water until officials notify you of its safety. Bring water to a rolling boil for a full 10 minutes or use chemicals (eight drops of chlorine bleach or iodine per gallon) or water purification tablets, as directed. Let the water sit at least 10 minutes before using. Water you saved in clean containers before the storm will be fine for 2-3 weeks. To be sure, add two drops of chlorine or iodine per gallon before drinking.

CLEAN-UP PRECAUTIONS

- ☐ Call professionals to remove large, uprooted trees, etc.
- ☐ Always use proper safety equipment such as heavy gloves, safety goggles, heavy boots, light- colored long-sleeve shirts and long pants.
- ☐ Tie back long hair, wear a hat and sunscreen.
- ☐ Drink plenty of fluids, rest and ask for help when you need it.
- ☐ Lift with the legs, not with the back.
- ☐ Don't burn trash.
- ☐ If you can't identify it, don't touch it.
- ☐ Be extremely careful with a chain saw and always heed safety warnings.

Source: Tampa Bay Regional Planning Council

Appendix 22

Flood Safety Checklist

If you are at risk from flooding, here are protective measures that need to be taken:

Preparatory Stage

☐ **KNOW YOUR RISK!**
Contact your insurance agent to determine if your business is in the 100-year or 500-year flood plain. If you do, purchase flood insurance! If you don't, consider purchasing flood insurance. More than 40% of all disaster flood loans are made to victims outside of the designated flood plain. Check your policy (ies) to ensure your business is adequately protected.

☐ **DISASTER SUPPLIES KIT**
Your kit may include a stock of food that requires no cooking/ refrigeration, but it should - at a minimum - have a first aid kit and weather alert radio.

☐ If you are vulnerable to flooding, consider acquiring sandbags or other materials to slow seepage into your building. Investigate other methods to reduce your risk of flooding including floodproofing, elevation or relocation.

☐ Have a plan to protect your records, equipment and files. Move valuable objects higher. Place them on shelves, tables and counter tops.

☐ Fuel your vehicle(s) and check oil and water.

AFTER THE FLOOD: SAFETY TIPS FOR EMPLOYEES

☐ Stay on higher ground until coast is clear.
☐ **DO NOT DRIVE ON A FLOODED ROAD**
☐ Don't attempt to wade in the water.
☐ Stay away from disaster areas.
☐ Do not handle live electrical equipment.
☐ Report downed power lines.
☐ Keep tuned to local stations for emergency information.

Source: Tampa Bay Regional Planning Council

Appendix 23

Tornado Safety Checklist

☐ Have a Weather Alert Radio in the office.

☐ Have a Plan to provide emergency notification (Warning System) to all employees, clients, visitors and customers in an emergency.

If a **Tornado Warning** is issued or if threatening severe weather approaches, make sure employees:

☐ Move to an interior room or hallway on the lowest floor and, if possible, get under a heavy piece of furniture.

☐ Stay away from windows.

☐ Mobile homes/ work trailers, even if tied down, offer little protection from tornadoes and should be abandoned.

☐ Occasionally, tornadoes develop so rapidly that advance warning is not possible. Remain alert for signs of an approaching tornado. Flying debris from tornadoes causes most deaths and injuries.

Source: Tampa Bay Regional Planning Council

Appendix 24

Lightning Safety Checklist

The chances of being struck by lightning are one in 600,000 but can be reduced by following safety rules. Most lightning deaths and injuries occur when people are caught outdoors. Make sure your employees know your policy regarding thunderstorm and lightning safety. And make sure employees' safety comes first. In recent years, people have been killed by lightning while: boating, swimming, golfing, bike riding, standing under a tree, riding on a lawnmower, talking on the telephone, loading a truck, playing sports, etc.

Lightning can strike anywhere!
Lightning Safety Tips

- ☐ Check the weather forecast before leaving for extended periods outdoors.
- ☐ Watch for signs of approaching storms.
- ☐ Postpone outdoor activities, if thunderstorms are imminent.
- ☐ Check on those who have trouble taking shelter if severe weather threatens.
- ☐ If you can hear thunder, seek shelter. Move to a sturdy building or car.
- ☐ Do not take shelter in small sheds, under isolated trees, or in a convertible.
- ☐ Get out of boats and pools and away from water.
- ☐ Do not use electrical appliances or the telephone unless it is cordless.
- ☐ If you feel your skin tingle or your hair stand on end, squat low to the ground on the balls of your feet. Place your hands on your knees with your head between them. Make yourself the smallest target possible and minimize your contact with the ground.

Source: Tampa Bay Regional Planning Council

Appendix 25

Wildfire Safety Checklist

PREVENTION: THE FLORIDA FIREWISE PROGRAM

Step 1. Choose a firewise location.

- ☐ Check with local officials to see what fire protection is available.
- ☐ Evaluate the site. A level area is better than a sloped one.
- ☐ Ensure that emergency vehicles will have easy access.
- ☐ Don't forget to clearly mark your location so firefighters can find you.

Step 2. Design and build firewise structures.

- ☐ Work with architects, contractors and fire officials to create a design that is both aesthetically pleasing and firewise.
- ☐ The number one cause of structural losses in wildland fires is from untreated wood shake roofs.
- ☐ Don't let sparks jump from your business or home to the wildland---or from a wildland fire to your home or business.

Step 3. Stay on guard with firewise landscaping and maintenance.

For specific information, go to www.firewise.org

EMERGENCY EVACUATION

- ☐ Implement the Warning Procedure to alert all employees of the danger and immediate evacuation.
- ☐ If there is sufficient time, take the vital records, i.e. server or backup tapes (in fire-proof container) to safer location. See "Go Box".
- ☐ Congregate at the appropriate meeting place outside of the building to verify all employees have evacuated the building.
- ☐ Confirm the Emergency Communications Plan (call-down procedures, emergency contact)
- ☐ If necessary, initiate the Continuity of Operations Plan (alternate work site(s), telework options, etc.)

Source: Tampa Bay Regional Planning Council

Sinkhole Action Checklist

☐ If a sinkhole forms on a street, mark and secure the sinkhole, and notify the agency responsible for maintenance, e.g. County Public Works Department; Municipal Public Works Department; Civic Association; or Private road maintained by adjacent property owners.

☐ If reported sinkhole is located on private property, mark and secure the area and determine if any structures are in danger. Indications of possible structural damage include - cracks in walls, floors, and pavement, and/or cracks in the ground surface.

☐ If structures are in possible danger:
A representative from the County Emergency Management Agency will respond to the scene and conduct a survey to determine if the structure is in danger or other hazards exist, and advise the business owner on contacting the appropriate agencies (i.e., insurance, utilities, phone, fire department).

☐ If the business is in danger, occupants will be advised that they should evacuate until assessment and repairs are made.

☐ The business owner must contact their insurance agent to send a claims representative out to assess the damage and make arrangements for repairs.

If it is determined that a sinkhole is on private property and **no structures are in danger**:

☐ Ensure that sinkhole is marked and secured. Make sure the sink is fenced, roped, or taped very clearly. Usually, the property owner will be liable if someone is hurt in the sinkhole.

☐ If lake or river levels are affected, or you think groundwater quality is endangered by a sinkhole, please report it to the Water Management District in your area.

☐ If your business is threatened, contact your insurance company.

☐ Check carefully for signs of the sinkhole enlarging, especially toward buildings, septic tanks, drain fields, and well (flowing water into a sinkhole will continue or accelerate its growth). This can be done with a thin hard metal rod that can be pushed into the soil. Areas near the sink will offer less resistance to the rod than the unaffected soil.

- ☐ Do not throw any waste into the sinkhole. Do not use the sinkhole as a drainage system. Pesticides and other wastes seep easily through the sinkhole into the aquifer - your drinking water.

- ☐ Do not construct buildings between sinkholes that form a line in a northwest-southeast or northeast-southwest direction.

- ☐ The county will not repair sinkholes on private property. If the hole is small, fill the hole with clean sand or dirt and monitor it for future growth.

- ☐ If the hole is large, contact your insurance agent and have them send a claims adjuster out to assess the damage and make arrangements for repairs.

- ☐ If desired, the business may make contact with a geo-technical engineering firm (private contractor) to evaluate the hole to officially determine if it is a sinkhole.

Source: Tampa Bay Regional Planning Council

Appendix 27

Extreme Heat Safety Checklist

- ☐ Stay indoors as much as possible.
  - If air conditioning is not available, stay on the lowest floor out of the sunshine.
  - Remember that electric fans do not cool; they just blow hot air around.
- ☐ Eat well-balanced, light and regular meals. Avoid using salt tablets unless directed to do so by a physician.
- ☐ Drink plenty of water regularly even if you do not feel thirsty.
  - Persons who have epilepsy or heart, kidney, or liver disease, are on fluid-restrictive diets, or have a problem with fluid retention should consult a doctor before increasing liquid intake.
- ☐ Limit intake of alcoholic beverages.
  - Although beer and alcoholic beverages appear to satisfy thirst, they actually cause further body dehydration.
- ☐ Never leave children or pets alone in closed vehicles.
- ☐ Dress in loose-fitting clothes that cover as much skin as possible.
  - Lightweight, light-colored clothing reflects heat and sunlight and helps maintain normal body temperature.
- ☐ Protect face and head by wearing a wide-brimmed hat.
- ☐ Avoid too much sunshine.
  - Sunburn slows the skin's ability to cool itself. Use a sunscreen lotion with a high SPF (sun protection factor) rating (i.e., 15 or greater).
- ☐ Avoid strenuous work during the warmest part of the day. Use a buddy system when working in extreme heat and take frequent breaks.
- ☐ Spend at least two hours per day in an air-conditioned place. If your home is not air conditioned, consider spending the warmest part of the day in public buildings such as libraries, schools, movie theaters, shopping malls and other community facilities.
- ☐ Check on family, friends, and neighbors who do not have air conditioning and who spend much of their time alone.

First-Aid For Heat-Induced Illnesses

1. Sunburn
   - *Symptoms:* Skin redness and pain, possible swelling, blisters, fever, headaches.
   - *First Aid:* Take a shower, using soap, to remove oils that may block pores, preventing the body from cooling naturally. If blisters occur, apply dry, sterile dressings and get medical attention.
2. Heat cramps
   - *Symptoms:* Painful spasms, usually in leg and abdominal muscles. Heavy sweating.
   - *First Aid:* Get the victim out to a cooler location. Lightly stretch and gently massage affected muscles to relieve spasm. Give sips of up to a half glass of cool water every 15 minutes. Do not give liquids with caffeine or alcohol. If nauseous, discontinue liquids.
3. Heat exhaustion
   - *Symptoms:* Heavy sweating and skin may be cool, pale or flushed. Weak pulse. Normal body temperature is possible but temperature will likely rise. Fainting or dizziness, nausea or vomiting, exhaustion and headaches are possible.
   - *First Aid:* Get victim to lie down in a cool place. Loosen or remove clothing. Apply cool, wet cloths. Fan or move victim to air-conditioned place. Give sips of water if victim is conscious. Be sure water is consumed slowly. Give half glass of cool water every 15 minutes. If nausea occurs, discontinue. If vomiting occurs, seek immediate medical attention.
4. Heat stroke (sun stroke)
   - *Symptoms:* High body temperature (105+). Hot, red, dry skin. Rapid, weak pulse; and rapid, shallow breathing. Possible unconsciousness. Victim will likely not sweat unless victim was sweating from recent strenuous activity.
   - *First Aid:* Heat stroke is a severe medical emergency. Call 911 or emergency medical services or get the victim to a hospital immediately. Delay can be fatal. Move victim to a cooler environment. Remove clothing. Try a cool bath, sponging or wet sheet to reduce body temperature. Watch for breathing problems. Use extreme caution. Use fans and air conditioners.

Source: Tampa Bay Regional Planning Council

Appendix 28

Water Conservation Checklist

Conserving water is very important during emergency water shortages. Water saved by one user may be enough to protect the critical needs of others. Irrigation practices can be changed to use less water or crops that use less water can be planted. Cities and towns can ration water, factories can change manufacturing methods, and individuals can practice water-saving measures to reduce consumption. If everyone reduces water use during a drought, more water will be available to share.

1. Practice indoor water conservation:

General

- Never pour water down the drain when there may be another use for it. Use it to water your indoor plants or garden.
- Repair dripping faucets by replacing washers. One drop per second wastes 2,700 gallons of water per year!

Bathroom

- Check all plumbing for leaks. Have leaks repaired by a plumber.
- Install a toilet displacement device to cut down on the amount of water needed to flush. Place a one-gallon plastic jug of water into the tank to displace toilet flow (do not use a brick, it may dissolve and loose pieces may cause damage to the internal parts). Be sure installation does not interfere with the operating parts.
- Consider purchasing a low-volume toilet that uses less than half the water of older models. NOTE: In many areas, low-volume units are required by law.
- Replace your showerhead with an ultra-low-flow version.
- Do not take baths—take short showers—only turn on water to get wet and lather and then again to rinse off.
- Place a bucket in the shower to catch excess water for watering plants.
- Don't let the water run while brushing your teeth, washing your face or shaving.
- Don't flush the toilet unnecessarily. Dispose of tissues, insects, and other similar waste in the trash rather than the toilet.

Kitchen

- Operate automatic dishwashers only when they are fully loaded. Use the "light wash" feature if available to use less water.
- Hand wash dishes by filling two containers—one with soapy water and the other with rinse water containing a small amount of chlorine bleach.
- Most dishwashers can clean soiled dishes very well, so dishes do not have to be rinsed before washing. Just remove large particles of food, and put the soiled dishes in the dishwasher.

- Store drinking water in the refrigerator. Don't let the tap run while you are waiting for water to cool.
- Do not waste water waiting for it to get hot. Capture it for other uses such as plant watering or heat it on the stove or in a microwave.
- Do not use running water to thaw meat or other frozen foods. Defrost food overnight in the refrigerator, or use the defrost setting on your microwave.
- Clean vegetables in a pan filled with water rather than running water from the tap.
- Kitchen sink disposals require a lot of water to operate properly. Start a compost pile as an alternate method of disposing of food waste, or simply dispose of food in the garbage.

Laundry

- Operate automatic clothes washers only when they are fully loaded or set the water level for the size of your load.

Long-term indoor water conservation

- Retrofit all household faucets by installing aerators with flow restrictors.
- Consider installing an instant hot water heater on your sink.
- Insulate your water pipes to reduce heat loss and prevent them from breaking if you have a sudden and unexpected spell of freezing weather.
- If you are considering installing a new heat pump or air-conditioning system, the new air-to-air models are just as efficient as the water-to-air type and do not waste water.
- Install a water-softening system only when the minerals in the water would damage your pipes. Turn the softener off while on vacation.
- When purchasing a new appliance, choose one that is more energy and water efficient.

2. Practice outdoor water conservation:

General

- If you have a well at home, check your pump periodically. If the automatic pump turns on and off while water is not being used, you have a leak.

Car washing

- Use a shut-off nozzle on your hose that can be adjusted down to a fine spray, so that water flows only as needed.
- Consider using a commercial car wash that recycles water. If you wash your own car, park on the grass so that you will be watering it at the same time.

Lawn Care

- Don't over water your lawn. A heavy rain eliminates the need for watering for up to two weeks. Most of the year, lawns only need one inch of water per week.
- Water in several short sessions rather than one long one in order for your lawn to better absorb moisture.
- Position sprinklers so water lands on the lawn and shrubs and not on paved areas.
- Avoid sprinklers that spray a fine mist. Mist can evaporate before it reaches the lawn. Check sprinkler systems and timing devices regularly to be sure they operate properly.

- Raise the lawn mower blade to at least three inches, or to its highest level. A higher cut encourages grass roots to grow deeper, shades the root system, and holds soil moisture.
- Plant drought-resistant lawn seed.
- Avoid over-fertilizing your lawn. Applying fertilizer increases the need for water. Apply fertilizers that contain slow-release, water-insoluble forms of nitrogen.
- Use a broom or blower instead of a hose to clean leaves and other debris from your driveway or sidewalk.
- Do not leave sprinklers or hoses unattended. A garden hose can pour out 600 gallons or more in only a few hours.

Pool

- Consider installing a new water-saving pool filter. A single back flushing with a traditional filter uses 180 to 250 gallons of water.
- Cover pools and spas to reduce evaporation of water.

Long term outdoor conservation

- Plant native and/or drought-tolerant grasses, ground covers, shrubs and trees. Once established, they do not need water as frequently and usually will survive a dry period without watering. Small plants require less water to become established. Group plants together based on similar water needs.
- Install irrigation devices that are the most water efficient for each use. Micro and drip irrigation and soaker hoses are examples of efficient devices.
- Use mulch to retain moisture in the soil. Mulch also helps control weeds that compete with landscape plants for water.
- Avoid purchasing recreational water toys that require a constant stream of water.
- Avoid installing ornamental water features (such as fountains) unless they use recycled water.

Participate in public water conservation programs of your local government, utility or water management district. Follow water conservation and water shortage rules in effect. Remember, you are included in the restrictions even if your water comes from a private well. Be sure to support community efforts that help develop and promote a water conservation ethic.

Contact your local water authority, utility district, or local emergency management agency for information specific to your area.

Source: Tampa Bay Regional Planning Council

Appendix 29

Winter Storm Safety Checklist

Preparedness is key to protecting your business, customers and employees. Again, be prepared to evacuate if flooding is imminent and advised by local officials and prepare a disaster supplies kit for your facility and call-down procedures for communicating with employees.

- ☐ If you are vulnerable to flooding, consider acquiring sandbags or other materials to slow seepage into your building. Investigate other methods to reduce your risk of flooding including floodproofing, elevation or relocation.
- ☐ Have a plan to protect your records, equipment and files. Move valuable objects higher. Place them on shelves, tables and counter tops.
- ☐ Fuel your vehicle(s) and check oil and water.
- ☐ If there is sufficient time, take the server or backup tapes (in fire-proof container) to safer location.
- ☐ Confirm the Emergency Communications Plan (call-down procedures, emergency contact)
- ☐ Secure your facility. Back up data files and take server(s) to more secure site. Unplug appliances. Protect equipment.
- ☐ Turn off the main water valve and electricity, if instructed to do so. Close and lock doors and windows.
- ☐ Leave early enough to (1) allow employees to secure their homes and purchase any needed emergency supplies, if appropriate, and (2) avoid being trapped by severe weather, other evacuation traffic, emergency response, etc.
- ☐ Follow recommended evacuation routes. Be alert.

Source: Tampa Bay Regional Planning Council

Appendix 30

Steps to Protect Your Farm from Terrorism

- ☐ **Talk seriously with your local police, fire and emergency departments.** Get to know them and let them know that you are making security a priority at your facility and will report any suspicious activities.

- ☐ **Make sure the appropriate public authorities have copies of maps of your facilities** that indicate service shut-off locations, security areas and any other areas of sensitivity or vulnerability.

- ☐ **Evaluate every request for information about your operation.** Never agree to an unusual request unless you have verified its validity. Whenever possible, require requests for sensitive information or tours to be in writing. Obtain as much information as possible—name, telephone number, address, reason for request, what the person will be doing with the information, who else has been contacted, etc. If anyone hesitates to cooperate with these requests, do not reveal information about or provide access to your operation.

- ☐ **Ask for references.** Make calls to verify that the person requesting any sensitive information is who he or she claims to be, especially if the person claims to be a reporter.

- ☐ **Ensure that access to your facility is controlled.** Establish check-in procedures for visitors. Require visitors to sign in and out upon entering and leaving the facility. Use visitor identification badges. This protects your visitor as well as you and your operation.

- ☐ **Escort visitors at all times while they are on the premises.** Employees should be instructed to report all unescorted visitors to the appropriate management and security personnel immediately.

- ☐ **Maintain basic security by locking office doors and file cabinets.** Have firewalls installed on your computer systems. Maintain separate business and personal computers. Keep all animal health products under lock and key. Use security lighting and alarms. Maintain fencing and gates. Post signs indicating restricted areas and no trespassing.

- ☐ **Thoroughly screen all job applicants.** Take the time to check all references. Double check anyone who shows a university or college identification card. Any hesitation by the prospective employee should exclude him or her from further consideration.

- ☐ **Watch for unusual behavior by new employees.** Pay attention to workers who stay unusually late, arrive unusually early, or access files, information, or other areas of the

facility outside their responsibility. Do not allow workers to remove documents from the site. Be suspicious of employees who ask questions on sensitive subjects or bring cameras or video equipment onsite. Watch for workers who are standoffish. Note the mode of dress (e.g., absence of leather or other animal products).

- ☐ **Tell all workers at hiring that unannounced locker checks are part of your routine security maintenance operation** and that your operation will report and file charges against any employee who breaks the law.

- ☐ **Inform employees in vulnerable areas that unauthorized surveillance or infiltration is a possibility**. Any suspicious activity should be reported to supervisors or the appropriate security person immediately.

- ☐ **Watch for warning signs that your operation may be a target.** Such signs can include an increase in requests for animal-specific information or on-farm tours, calls and letters questioning or criticizing your business or particular practices, any harassing calls and letters to you or a nearby operation, increase in media attention to issues relating to the livestock industry, special interest group campaigns locally, and unusual interest in gaining employment.

- ☐ **Develop a company statement concerning care, treatment and nutrition for your animals.** Designate a single spokesperson to handle all calls about animal care, animal rights or any company policy concerning animals.

- ☐ **Conduct routine tests** of your security system and, if necessary, mock drills on your response procedures.

- ☐ **Develop a crisis communication and action plan.** Establish policies and procedures for handling disruptive and illegal situations, as well as for handling adverse publicity that might result. In developing response procedures, remember that steps to protect people should take priority over steps to protect property.

Source: American Farm Bureau. "Steps to Protect Your Farm from Terrorism," *The Voice of Agriculture Newsroom*, October 22, 2001. Accessed at www.fb.org/news/fbn/html/agriculturalterrorism.html.

Source: Tampa Bay Regional Planning Council

Appendix 31

What To Do During and After a Hazardous Material Incident

IF YOU'RE TOLD TO EVACUATE

- ☐ You should move to the place/shelter designated by public officials. Listen to your radio and TV for specific instructions.
- ☐ Stay as calm as you can. If you already know where to go and what to take, that will help.
- ☐ Quickly gather what you will need, unless you are told to leave immediately.
- ☐ Turn off lights, heating, cooling, and ventilation systems & lock your building.
- ☐ Carpool if possible.
- ☐ Keep car windows/air vents closed. Do not use the air conditioner until you are out of the evacuation area.
- ☐ Drive safely - Law enforcement officers will help with traffic control.
- ☐ Do not worry about your property while you are away. The area will be secured.

YOUR CHILDREN

Employees will be concerned for their children. Reassure them that if children are in school at the time the evacuation is ordered, school officials will take care of them. If students have to leave their schools for a safer shelter, **they will be the first to move.**

Parents should not try to call or go to the children's school to pick them up - that could delay their evacuation to a safer area. Teachers and other adults will take them to a designated place or shelter. In some cases, the school may not be at risk to the chemical release. Either way, you and your employees will be told by local officials through radio and TV where to pick up the children after they have been evacuated.

IF YOU ARE TOLD TO STAY INDOORS AND *SHELTER IN PLACE*

Stay inside the facility. This action will be recommended if there is a short release, a small amount of hazardous material in the air, or if time does not permit evacuation before the arrival of a cloud of toxic vapor. Take these steps to protect yourself and employees:

- ☐ Stay inside until local officials say you can leave safely. This will most likely be for no more than a few hours.
- ☐ **If your business has animals, if possible bring them indoors!**
- ☐ Close all doors and windows.
- ☐ Seal all gaps under doorways and windows with damp towels and duct tape.
- ☐ Turn off heating, cooling or ventilation systems.
- ☐ Listen to your local radio or TV stations for further instructions.
- ☐ Resist the impulse to go outdoors and "check things out" before given the "All Clear" by authorities.
- ☐ If you are told to protect your breathing, cover your nose and mouth with a damp handkerchief or other cloth folded over several times.

WHEN YOU RETURN TO YOUR BUSINESS, WHAT PRECAUTIONS SHOULD YOU TAKE?

Officials will notify you as to what precautions need to be taken. Depending of the type of chemical, you may need to do the following:

- ☐ Wash all dishes and eating utensils.
- ☐ Dispose of any open food, etc.
- ☐ Vacuum furniture, floors, other items.
- ☐ Change air conditioner filters.
- ☐ Air out files, copy paper, etc.
- ☐ Purify water before using.

Source: Tampa Bay Regional Planning Council

Appendix 32

Fire Safety Checklist

When OSHA conducts workplace inspections, it checks to see whether employers are complying with OSHA standards for fire safety:

Employee Training

☐ OSHA standards require employers to provide proper exits, fire fighting equipment, emergency plans, and employee training to prevent fire deaths and injuries in the workplace.

Building Fire Exits

☐ Each workplace building must have at least two means of escape remote from each other to be used in a fire emergency.

☐ Fire doors must not be blocked or locked to prevent emergency use when employees are within the buildings.

☐ Delayed opening of fire doors is permitted when an approved alarm system is integrated into the fire door design.

☐ Exit routes from buildings must be clear and free of obstructions and properly marked with signs designating exits from the building.

Portable Fire Extinguishers

☐ Each workplace building must have a full complement of the proper type of fire extinguisher for the fire hazards present.

☐ Employees expected or anticipated to use fire extinguishers must be instructed on the hazards of fighting fire, how to properly operate the fire extinguishers available, and what procedures to follow in alerting others to the fire emergency.

☐ Only approved fire extinguishers are permitted to be used in workplaces, and they must be kept in good operating condition. Proper maintenance and inspection of this equipment is required of each employer.

☐ Where the employer wishes to evacuate employees instead of having them fight small fires there must be written emergency plans and employee training for proper evacuation.

Emergency Evacuation Planning

- ☐ Each employer needs to have a written emergency action plan for evacuation of employees which describes the routes to use and procedures to be followed by employees. Also, procedures for accounting for all evacuated employees must be part of the plan. The written plan must be available for employee review.

- ☐ Where needed, special procedures for helping physically impaired employees must be addressed in the plan; also, the plan must include procedures for those employees who must remain behind temporarily to shut down critical plant equipment before they evacuate.

- ☐ The preferred means of alerting employees to a fire emergency must be part of the plan and an employee alarm system must be available throughout the workplace complex and must be used for emergency alerting for evacuation. The alarm system may be voice communication or sound signals such as bells, whistles or horns. Employees must know the evacuation signal.

- ☐ Training of all employees in what is to be done in an emergency is required. Employers must review the plan with newly assigned employees so they know correct actions in an emergency and with all employees when the plan is changed.

Fire Prevention Plan

- ☐ Employers need to implement a written fire prevention plan to complement the fire evacuation plan to minimize the frequency of evacuation. Stopping unwanted fires from occurring is the most efficient way to handle them. The written plan shall be available for employee review.

- ☐ Housekeeping procedures for storage and cleanup of flammable materials and flammable waste must be included in the plan. Recycling of flammable waste such as paper is encouraged; however, handling and packaging procedures must be included in the plan.

- ☐ Procedures for controlling workplace ignition sources such as smoking, welding and burning must be addressed in the plan. Heat producing equipment such as burners, heat exchangers, boilers, ovens, stoves, fryers, etc., must be properly maintained and kept clean of accumulations of flammable residues; flammables are not to be stored close to these pieces of equipment.

- ☐ All employees are to be apprized of the potential fire hazards of their job and the procedures called for in the employer's fire prevention plan. The plan shall be

reviewed with all new employees when they begin their job and with all employees when the plan is changed.

Fire Suppression System

- ☐ Properly designed and installed fixed fire suppression systems enhance fire safety in the workplace. Automatic sprinkler systems throughout the workplace are among the most reliable fire fighting means. The fire sprinkler system detects the fire, sounds an alarm and puts the water where the fire and heat are located.

- ☐ Automatic fire suppression systems require proper maintenance to keep them in serviceable condition. When it is necessary to take a fire suppression system out of service while business continues, the employer must temporarily substitute a fire watch of trained employees standing by to respond quickly to any fire emergency in the normally protected area. The fire watch must interface with the employers' fire prevention plan and emergency action plan.

- ☐ Signs must be posted about areas protected by total flooding fire suppression systems which use agents that are a serious health hazard such as carbon dioxide, Halon 1211, etc. Such automatic systems must be equipped with area pre-discharge alarm systems to warn employees of the impending discharge of the system and allow time to evacuate the area. There must be an emergency action plan to provide for the safe evacuation of employees from within the protected area. Such plans are to be part of the overall evacuation plan for the workplace facility.

This is one of a series of fact sheets highlighting U.S. Department of Labor programs. It is intended as a general description only and does not carry the force of legal opinion. This information will be made available to sensory impaired individuals upon request. Voice phone: (202) 523-8151. TDD message referral phone: 1-800-326-2577.

Source: Tampa Bay Regional Planning Council

Appendix 33

Tips for Fire Prevention for Small Business

By: Captain Bud Gundersen

These few simple precautions can go a long way toward preventing a hostile fire from destroying your business:

FIRE EXTINGUISHERS:

☐ Every business location is required to have at least one extinguisher. Required extinguishers must be serviced yearly, or immediately after use, by a person having a valid certificate. Extinguishers must be installed on approved brackets or set in a fire department approved cabinet. They must be conspicuously located or have signs which identify the location. Please contact your local fire station if you have any questions regarding the size, type, or placement of extinguishers.

A FEW MORE TIPS...

Water Heaters: The burner flame can easily start a fire if flammable items are placed too close. Maintain at least three feet of clearance around your hot water heater.

Electrical Panels: In the event of a fire, three feet of clearance around the electrical panel is necessary to access circuit breakers.

Exit Aisles: Must be clear of storage at all times.

Fire Control Valves: Often located in obscure areas of buildings, fire control valves can get blocked by storage. Maintain a three-foot access aisle and make sure that the valves are well marked.

ELECTRICAL HAZARDS:

☐ Extension cords are often misused and can be very hazardous. They should be used only for temporary wiring, not permanent use. They should not be run through ceilings, walls, doors or windows. Also, beware of the extension cord "octopus." Using multiple outlet adapters to run numerous items off a single outlet can be dangerous. It is much safer to install additional outlets rather than to use adapters and extension cords.

EXIT DOORS:

☐ For security purposes many business owners lock rear exit doors. Even in a small shop, someone can be trapped by a fire and need to rely on the rear door to escape. All required exit doors must be unlocked during business hours or have escape hardware which allows them to be opened from the inside without a key. This is a crucial issue to life safety. Both security and fire safety can be accommodated by installing escape hardware or a door alarm.

ADDRESS NUMBERS:

☐ Make sure that your address is clearly visible from the street. If you have a fire or medical emergency, the fire department wants to find you fast. It is also very helpful if someone can wait for them out on the street and flag them in.

DATA BACK-UP:

☐ While protecting your employees will always be your first priority, mitigation of business loss will include more than fire extinguishers, sprinkler systems and quick fire response. Your business needs to protect its records and data files. Our reliance on electronic data makes data protection a major concern for your business survival. Even in small businesses, it is crucial to back-up your data files at least once a week.

FIRE-PROOF SAFES:

☐ Keep a copy of your electronic files and critical data/ information in a fire-resistant safe. If you are in a hurricane evacuation zone, flood zone or vulnerable to other areas, then an alternate site (outside of the vulnerability zone) should be selected and a fire-resistant safe kept there for keeping records during a potential evacuation.

Source: Tampa Bay Regional Planning Council

Power Service Disruption Checklist

Power Service Disruption could be the result of a weather event, an accident or a terrorist attack. There are some physical measures a business can take to be prepared for power Service Disruptions. (i.e., surge protectors or backup generation for critical equipment). As in the case of any other emergency, the business needs to address liabilities, risks and response activities in advance. An emergency plan can include some of the following measures.

Facility

- ☐ If your lights fail, first try checking your breakers or fuses. Re-setting the breakers or putting in new fuses may bring your lights back on. To reset a breaker, turn it to the OFF position, press firmly off, then push to the ON position. If re-setting the breaker or replacing the fuses doesn't help, call your local electric utility.
- ☐ Post phone number for local electric utility at appropriate locations.
- ☐ If using back-up generation, what are your procedures to avoid "backfeed".

Medical Emergency

In the case of a medical emergency during a power outage, employees should seek immediate care at the nearest appropriate health care facility. Please note that some telephones require electricity and may not be in service during an outage. Businesses are encouraged to have a back-up communication plan in case of such an event. When requesting emergency assistance, location finding devices such as GPS can be very useful during an event that changes the landscape.

Facility Protection and Security

- ☐ Even if people do not know whether radioactive materials were present, following these simple steps can help reduce their injury from other chemicals that might have been present in the blast.
- ☐ Determine your threat level and communicate to employees.
- ☐ Employers are encouraged to develop a business security plan. Included in this plan should be security processes dealing with power outages/disruptions. Need for security guards because your alarm system is not functioning?
- ☐ Be on the alert for fires and call authorities if smoke or fire is spotted.
- ☐ What to do if you have another emergency during the outage (e.g., material spill).
- ☐ What to do if water enters your facility. What equipment could you use when the lights come back on?
- ☐ Procedure for re-entering the building.

Employee Field Work

- ☐ Inform personnel that any fallen wire is potentially hazardous. *(See Stay Safe this Storm Season* pamphlet*)*
- ☐ Inform personnel how to deal with a situation of a fallen power line on their car.

Communications

- ☐ Inform the employees how they will be communicating with their immediate supervisor or employer if they are in the field during a large scale power outage.
- ☐ Publish a telephone number to be used by employees to call their supervisor and be prepared to provide reporting instructions.
- ☐ Make appropriate communication to your customers.

Source: Tampa Bay Regional Planning Council

Appendix 35

Bomb Threat Procedures

- ☐ If you receive a bomb threat by phone, instruct employee(s) to get as much information from the caller as possible. Keep the caller on the line and record everything that is said.

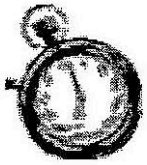
- ☐ If you are notified of a bomb threat referring to a delivered package, do not touch any suspicious packages. Clear the area around the suspicious packages and notify the police immediately.

- ☐ At the same time, emergency warning procedure should be implemented, so others can notify law enforcement, building management and staff.

- ☐ Initiate shutdown and emergency evacuation procedures.

- ☐ At meeting place, verify the evacuation of all employees and visitors.

Bomb Threat Checklist



KEEP THE CALLER ON THE LINE AS LONG AS POSSIBLE!

EXACT TIME AND DATE OF CALL:_____

EXACT WORDS OF CALLER:_____

_____

Voice

- ☐ Loud
- ☐ High Pitched
- ☐ Raspy
- ☐ Intoxicated
- ☐ Soft
- ☐ Deep
- ☐ Pleasant
- ☐ Other

Language

- ☐ Excellent
- ☐ Fair
- ☐ Foul

- ☐ Good
- ☐ Poor
- ☐ Other

Accent

- ☐ Local
- ☐ Foreign
- ☐ Race
- ☐ Not Local
- ☐ Region

Speech

- ☐ Fast
- ☐ Distinct
- ☐ Stutter
- ☐ Slurred
- ☐ Slow

- ☐ Distorted
- ☐ Nasal
- ☐ Lisp
- ☐ Other

Manner

- ☐ Calm
- ☐ Rational
- ☐ Coherent
- ☐ Deliberate
- ☐ Righteous
- ☐ Angry
- ☐ Irrational
- ☐ Incoherent
- ☐ Emotional
- ☐ Laughing

Familiarity With Threatened Facility ?

- ☐ Much
- ☐ Some
- ☐ None

Background Noise

- ☐ Factory Machines
- ☐ Bedlam
- ☐ Music
- ☐ Office Machines
- ☐ Mixed
- ☐ Street Traffic
- ☐ Trains
- ☐ Animals
- ☐ Quiet
- ☐ Voices
- ☐ Airplanes
- ☐ Party Atmosphere

Questions to Ask the Caller

1. **When is the bomb going to explode?**

   _____

2. **Where is the bomb?**

   _____

3. **What does it look like?**

   _____

4. **What kind of bomb is it?**

   _____

5. **What will cause it to explode?**

   _____

6. **Did you place the bomb?**

   _____

7. **Why did you place the bomb?**

   _____

8. **Where are you calling from?**

   _____

9. **What is your address?**

   _____

10. **What is your name?**

    _____

If voice is familiar, whom did it sound like?

_____

Were there any background noises?

_____

Telephone number call received at:

_____

Person receiving call:

_____

Any Additional remarks:

_____

DIAL 911 IMMEDIATELY AND REPORT THREAT

Source: Tampa Bay Regional Planning Council

Checklist to Prepare and Respond to a Chemical/Biological Attack

- ☐ Assemble a disaster supply kit (see the "Emergency Planning and Disaster Supplies" chapter for more information) and be sure to include:
- ☐ Battery-powered commercial radio with extra batteries.
- ☐ Non-perishable food and drinking water.
- ☐ Roll of duct tape and scissors.
- ☐ Plastic for doors, windows and vents for the room in which you will shelter in place—this should be an internal room where you can block out air that may contain hazardous chemical or biological agents. To save critical time during an emergency, sheeting should be pre-measured and cut for each opening.
- ☐ First aid kit.
- ☐ Sanitation supplies including soap, water and bleach.

What to do during a chemical or biological attack

- ☐ Listen to your radio for instructions from authorities such as whether to remain inside or to evacuate.
- ☐ If you are instructed to remain in your home, the building where you are, or other shelter during a chemical or biological attack:
- ☐ Turn off all ventilation, including furnaces, air conditioners, vents and fans.
- ☐ Seek shelter in an internal room, preferably one without windows. Seal the room with duct tape and plastic sheeting. Ten square feet of floor space per person will provide sufficient air to prevent carbon dioxide build-up for up to five hours. (See "Shelter in Place" Checklist)
- ☐ Remain in protected areas where toxic vapors are reduced or eliminated, and be sure to take your battery-operated radio with you.

If you are caught in an unprotected area, you should:

- ☐ Attempt to get up-wind of the contaminated area.
- ☐ Attempt to find shelter as quickly as possible.
- ☐ Listen to your radio for official instructions.

What to do after a chemical attack

Immediate symptoms of exposure to chemical agents may include blurred vision, eye irritation, difficulty breathing and nausea. A person affected by a chemical or biological agent requires immediate attention by professional medical personnel. If medical help is not immediately available, decontaminate yourself and assist in decontaminating others. Decontamination is needed within minutes of exposure to minimize health consequences. (However, you should not leave the safety of a shelter to go outdoors to help others until authorities announce it is safe to do so.)

Use extreme caution when helping others who have been exposed to chemical agents:

- ☐ Remove all clothing and other items in contact with the body. Contaminated clothing normally removed over the head should be cut off to avoid contact with the eyes, nose, and mouth. Put into a plastic bag if possible. Decontaminate hands using soap and water. Remove eyeglasses or contact lenses. Put glasses in a pan of household bleach to decontaminate.
- ☐ Remove all items in contact with the body.
- ☐ Flush eyes with lots of water.
- ☐ Gently wash face and hair with soap and water; then thoroughly rinse with water.
- ☐ Decontaminate other body areas likely to have been contaminated. Blot (do not swab or scrape) with a cloth soaked in soapy water and rinse with clear water.
- ☐ Change into uncontaminated clothes. Clothing stored in drawers or closets is likely to be uncontaminated.
- ☐ If possible, proceed to a medical facility for screening.

What to do after a biological attack

In many biological attacks, people will not know they have been exposed to an agent. In such situations, the first evidence of an attack may be when you notice symptoms of the disease caused by an agent exposure, and you should seek immediate medical attention for treatment.

In some situations, like the anthrax letters sent in 2001, people may be alerted to a potential exposure. If this is the case, pay close attention to all official warnings and instructions on how to proceed. The delivery of medical services for a biological event may be handled differently to respond to increased demand. Again, it will be important for you to pay attention to official instructions via radio, television, and emergency alert systems.

If your skin or clothing comes in contact with a visible, potentially infectious substance, you should remove and bag your clothes and personal items and wash yourself with warm soapy water immediately. Put on clean clothes and seek medical assistance.

For more information, visit the website for the Centers for Disease Control and Prevention, www.bt.cdc.gov.

Source: Tampa Bay Regional Planning Council

Appendix 37

Handling Suspicious Parcels or Letters

Be wary of suspicious packages and letters. They can contain explosives, chemical or biological agents. Be particularly cautious at your place of employment.

Some typical characteristics postal inspectors have detected over the years, which ought to trigger suspicion, include parcels that—

- Are unexpected or from someone unfamiliar to you.
- Have no return address, or have one that can't be verified as legitimate.
- Are marked with restrictive endorsements, such as "Personal," "Confidential" or "Do not x-ray."
- Have protruding wires or aluminum foil, strange odors or stains.
- Show a city or state in the postmark that doesn't match the return address.
- Are of unusual weight, given their size, or are lopsided or oddly shaped.
- Are marked with any threatening language.
- Have inappropriate or unusual labeling.
- Have excessive postage or excessive packaging material such as masking tape and string.
- Have misspellings of common words.
- Are addressed to someone no longer with your organization or are otherwise outdated.
- Have incorrect titles or title without a name.
- Are not addressed to a specific person.
- Have handwritten or poorly typed addresses.

With suspicious envelopes and packages other than those that might contain explosives, take these additional steps against possible biological and chemical agents.

- Refrain from eating or drinking in a designated mail handling area.
- Place suspicious envelopes or packages in a plastic bag or some other type of container to prevent leakage of contents. Never sniff or smell suspect mail.
- If you do not have a container, then cover the envelope or package with anything available (e.g., clothing, paper, trash can, etc.) and do not remove the cover.
- Leave the room and close the door, or section off the area Wash your hands with soap and water to prevent spreading any powder to your face.
- If you are at work, report the incident to your building security official or an available supervisor, who should notify police and other authorities without delay.
- List all people who were in the room or area when this suspicious letter or package was recognized. Give a copy of this list to both the local public health authorities and law enforcement officials for follow-up investigations and advice.
- If you are at home, report the incident to local police.

Source: Tampa Bay Regional Planning Council

Appendix 38

Radiological Emergency Safety Checklist

Immediate Precautions

- ☐ Notify your Facility Radiation Safety Officer (if applicable), 911, the local authorities and Radiation Control Authority on Accident Conditions. Follow applicable permit and regulatory requirements.
- ☐ Notify 911 of the possible presence of radioactive materials
- ☐ Isolate hazard area in accordance with your As Low As Reasonably Achievable (ALARA) plan and restrict access.
- ☐ Do Not Touch containers.
- ☐ Upon arrival of Law Enforcement or Fire Department, inform the First Responder that radioactivity may be present.
- ☐ In the case of fire, Do Not attempt to move containers out of fire zone. Retreat to a safe area and wait for Local Authorities. Please note, radioactivity does not change flammability or properties of other materials.
- ☐ In the case of a medical emergency, use First Aid treatment according to the nature of the injury.
- ☐ Advise medical personnel that victim may be contaminated with radioactive material.
- ☐ Detain persons exposed to Radioactive Material until arrival or instruction of Radiation Control Authority. Potential route of exposure can include Inhalation, Ingestion, or Breaks in Skin.
- ☐ Include business specific information in your emergency plans. Inform the employees regarding radiation safety. Follow your ALARA plan. Publish a telephone number to be used by employees to call their supervisor and be prepared to provide reporting instructions.

Source: Tampa Bay Regional Planning Council

Appendix 39

Radiological Emergency: Immediate Precautions in the Case of a Terrorist Attack

Radiation cannot be seen, smelled, felt, or tasted by humans. Therefore, if people are present at the scene of an explosion, they will not know whether radioactive materials were involved at the time of the explosion. However, following these simple steps can help reduce their injury from other chemicals that might have been present in the blast.

If people are not too severely injured by the initial blast, they should:

- ☐ Leave the immediate area on foot. Do not panic. Do not take public or private transportation such as buses, subways, or cars because if radioactive materials were involved, they may contaminate cars or the public transportation system.
- ☐ Go inside the nearest building. Staying inside will reduce people's exposure to any radioactive material that may be on dust at the scene.
- ☐ Remove their clothes as soon as possible, place them in a plastic bag, and seal it. Removing clothing will remove most of the contamination caused by external exposure to radioactive materials. Saving the contaminated clothing would allow testing for exposure without invasive sampling.
- ☐ Take a shower or wash themselves as best they can. Washing will reduce the amount of radioactive contamination on the body and will effectively reduce total exposure.
- ☐ Be on the lookout for information. Once emergency personnel can assess the scene and the damage, they will be able to tell people whether radiation was involved.

Note:
There are many questions regarding the likelihood of whether terrorists would use radioactive materials in attacks since radioactive materials are hard to handle and the impact to the public would not be as tangible or visible after an attack. Different methods can be used in a radiological terrorist attack. A weapon could include explosion as a mechanism to disperse radiation as in the case of a dirty bomb or it could be more "passive" and include exposing the public to radioactive sources from gauges used in industry or to radioactive waste.

Source: Tampa Bay Regional Planning Council

Appendix 40

Prevention and Response To Workplace Violence

- ☐ Establish an atmosphere of awareness and encourage employees to report suspicious activity or behavior, strangers, unexplained events, unscheduled deliveries or suspicious mail;
- ☐ Maintain strict hiring policies that include background checks;
- ☐ Establish written workplace anti-violence policies and security procedures with zero tolerance for any instance of violence;
- ☐ List prohibited conduct;
- ☐ Monitor current employees' behavior;
- ☐ Train managers and supervisors how to recognize and resolve problems;
- ☐ Maintain a working environment that is open to communication and respectful to all employees; and
- ☐ Balance a violence-free workplace with employee rights.
- ☐ If you find yourself struggling to wade through these complicated laws, you may want to consult an employment law attorney.
- ☐ Institute appropriate security procedures to prevent attacks on the facility or your employees, by restricting access to your facility and incorporating crime prevention techniques;
- ☐ Establish a procedure to alert management and staff and law enforcement of a potential threat ("panic button," intercom, code word)
- ☐ Ensure all employees understand the Emergency Evacuation Procedures.

Source: Tampa Bay Regional Planning Council

Appendix 41
Mission Essential Function Survey

1 Mission Essential Function	2 Justification	3 Time Period	4 Min. Staff	5 Special Equipment	6 Space Needs	7 Plan (Y/N)	8 Business Manager

Survey Questions

1. List your mission essential activities or functions in priority order.
2. Provide your justification for determining the functions to be mission essential.
3. For each mission essential function identify the critical restoration time period (e.g., 24 hours, 3 days, 2 weeks, etc.).
4. Identify the minimum of staff needed to operate at a relocation site for each mission essential function.
5. Identify any special equipment, etc., that must be relocated in support of a mission essential function to help determine space requirements.
6. Identify by name, position and telephone number your Continuity of Operations "business manager."

Source: Tampa Bay Regional Planning Council

Appendix 42

CRITICAL INCIDENT STRESS INFORMATION SHEETS

You have experienced a traumatic event or a critical incident (any event that causes unusually strong emotional reactions that have the potential to interfere with the ability to function normally). Even though the event may be over, you may now be experiencing or may experience later, some strong emotional or physical reactions. It is very common, in fact quite *normal*, for people to experience emotional aftershocks when they have passed through a horrible event.

Sometimes the emotional aftershocks (or stress reactions) appear immediately after the traumatic event. Sometimes they may appear a few hours or a few days later. And, in some cases, weeks or months may pass before the stress reactions appear.

The signs and symptoms of a stress reaction may last a few days, a few weeks, a few months, or longer, depending on the severity of the traumatic event. The understanding and the support of loved ones usually cause the stress reactions to pass more quickly. Occasionally, the traumatic event is so painful that professional assistance may be necessary. This does not imply craziness or weakness. It simply indicates that the particular event was just too powerful for the person to manage by himself.

Here are some common signs and signals of a stress reaction:

Physical*	***Cognitive***	***Emotional***	***Behavioral***
chills	confusion	fear	withdrawal
thirst	nightmares	guilt	antisocial acts
fatigue	uncertainty	grief	inability to rest
nausea	hypervigilance	panic	intensified pacing
fainting	suspiciousness	denial	erratic movements
twitches	intrusive images	anxiety	change in social activity
vomiting	blaming someone	agitation	change in speech patterns
dizziness	poor problem solving	irritability	loss or increase of appetite
weakness	poor abstract thinking	depression	hyperalert to environment
chest pain	poor attention/ decisions	intense anger	increased alcohol consumption
headaches	poor concentration/memory	apprehension	change in usual communications
elevated BP	disorientation of time, place or person	emotional shock	etc...
rapid heart rate	difficulty identifying objects or people	emotional outbursts	
muscle tremors	heightened or lowered alertness	feeling overwhelmed	
shock symptoms	increased or decreased awareness of surroundings	loss of emotional control	
grinding of teeth	etc...	inappropriate emotional response	
visual difficulties		etc...	
profuse sweating			
difficulty breathing			
etc...			

**** Any of these symtoms may indicate the need for medical evaluation. When in doubt, contact a physician.***

THINGS TO TRY:

- WITHIN THE FIRST 24 - 48 HOURS periods of appropriate physical exercise, alternated with relaxation will alleviate some of the physical reactions.
- Structure your time; keep busy.
- You're normal and having normal reactions; don't label yourself crazy.
- Talk to people; talk is the most healing medicine.
- Be aware of *numbing* the pain with overuse of drugs or alcohol, you don't need to complicate this with a substance abuse problem.
- Reach out; people do care.
- Maintain as normal a schedule as possible.
- Spend time with others.
- Help your co-workers as much as possible by sharing feelings and checking out how they are doing.
- Give yourself permission to feel rotten and share your feelings with others.
- Keep a journal; write your way through those sleepless hours.
- Do things that feel good to you.
- Realize those around you are under stress.
- Don't make any big life changes.
- Do make as many daily decisions as possible that will give you a feeling of control over your life, i.e., if someone asks you what you want to eat, answer him even if you're not sure.
- Get plenty of rest.
- Don't try to fight reoccurring thoughts, dreams or flashbacks - they are normal and will decrease over time and become less painful.
- Eat well-balanced and regular meals (even if you don't feel like it).

FOR FAMILY MEMBERS & FRIENDS

- Listen carefully.
- Spend time with the traumatized person.
- Offer your assistance and a listening ear if (s)he has not asked for help.
- Reassure him that he is safe.
- Help him with everyday tasks like cleaning, cooking, caring for the family, minding children.
- Give him some private time.
- Don't take his anger or other feelings personally.
- Don't tell him that he is "lucky it wasn't worse;" a traumatized person is not consoled by those statements. Instead, tell him that you are sorry such an event has occurred and you want to understand and assist him.

Appendix 43

Florida Statutes Regarding Volunteers

Definition Of Volunteer As Defined Under Florida Statute 125.9501:

(1) "Volunteer" means a person who, of his or her own free will, provides goods or services to any unit of county government or to any constitutional county officer without receiving monetary or material compensation.

(2) "Regular-service volunteer" means a person engaged in specific voluntary service activities on an ongoing or continual basis.

(3) "Occasional-service volunteer" means a person who offers to provide a one-time or occasional voluntary service.

Good Samaritan Act: Immunity from Civil Liability as Defined under Florida Statute 798.13:

Any person, including those licensed to practice medicine, who gratuitously and in good faith renders emergency care or treatment either in direct response to emergency situations related to and arising out of a State of Emergency which has been declared pursuant to Florida Statute 252.36 or at the scene of an emergency outside of a hospital, doctor's office, or other place having proper medical equipment, without objection of the injured victim or victims thereof, shall not be held liable for civil damages as a result of any act or failure to act in providing or arranging further medical treatment where the person acts as an ordinary reasonably prudent person would have acted under the same or similar circumstances.

Florida Volunteer Protection Act as Defined under Florida Statute 768.1355:

(1) Any person who volunteers to perform any service for any nonprofit organization, including an officer or director of such organization, without compensation, except reimbursement for actual expenses, shall be considered an agent of such nonprofit organization when acting within the scope of any official duties performed under such volunteer services. Such person shall incur no civil liability for any act or omission by such person which results in personal injury or property damage if:

   (a) Such person was acting in good faith within the scope of any official duties performed under such volunteer service and such person was acting as an ordinary reasonably prudent person would have acted under the same or similar circumstances; and
   (b) The injury or damage was not caused by any wanton or willful misconduct on the part of such person in the performance of such duties.