MFSA

MAILING & FULFILLMENT
SERVICE ASSOCIATION

Disaster Preparedness & Business Continuity Planning

©2007

MFSA Disaster Preparedness & Business Continuity Planning

I. ***Introduction***

II. ***Disaster Planning***

III. ***Creating Your Plan***

IV. ***Appendix: Additional Resources***

I. Introduction

About This Document

This MSFA Disaster Recovery and Business Continuity Preparedness document explains the points an organization needs to consider when preparing its own disaster recovery plan that will allow the business to resume operations quickly following a disruption.

Preparing a comprehensive customized disaster recovery plan requires research and discussions among key staff members to address specific issues and concerns. Each organization's circumstances and structures are unique, so a plan will have to be tailored to suit its needs. It is important to recognize that there is no "magic" plan that an organization can purchase that will provide all the answers or software that will create a viable plan for them with just a few keystrokes. No document will address every situation and circumstance. But there are templates and sample plans available from state and Federal government organizations that will provide a good starting point for disaster preparation.

Conceivably an organization could share its plan with another organization for ideas on how to formulate a plan; however, some plans may include confidential information that should not be made available to those outside the organization.

Take this document and use it as you wish: cut and paste those sections that are applicable, expand where needed. Assign specific staff to complete the various sections, take a copy home...store it on your intranet...give copies to key personnel, including the board chair, the secretary or other appropriate board members.

When you begin to create your Disaster Recovery and Business Continuity plan, don't become overwhelmed by the magnitude of the task ahead. Divide the plan into sections and prioritize them, working first on the sections that are most important (for example, personnel, computer/IT, etc.), and move through the process as time allows. When it comes to disaster recovery, even the most incomplete plan is better than no plan at all. Above all, the most important thing is to make some plans that can be implemented quickly in the event of an interruption.

IMPORTANT: The Mailing & Fulfillment Service Association ("MFSA") is a nonprofit corporation, which is exempt from federal taxation under Section 501(c)(6) of the Internal Revenue Code. This Guide is a publication of MFSA and it has been developed in furtherance of MFSA's nonprofit and tax exempt purposes. MFSA has taken reasonable measures to develop this publication in a fair, reasonable, open, unbiased, and objective manner for the purpose of informing MFSA members and others of the best practices in disaster preparedness and business continuity planning. The guidelines contained in this Guide are simply suggested; the adherence to or following of such guidelines is strictly voluntary. Additionally, the nature of appropriate practices or guidance is likely to change over time and with developments in technology. MFSA cannot guarantee the accuracy, completeness, efficacy, or timeliness of this publication. Use of this publication is voluntary, and reliance on the material contained within the publication should be undertaken only after an independent review by the user. Inclusion of material in this publication does not constitute a guarantee, warranty, or endorsement by MFSA regarding any guidance, methodologies, or practices, and does not constitute any guarantee, warranty, endorsement, or sponsorship of or by any company or company product that may be referenced. Further, neither MFSA nor the Nonprofit Coordinating Committee of New York, their officers, directors, members, employees, agents, or volunteers that contributed material to this publication shall be liable for any loss, damage, or claim with respect to any such documents, work, or services; all such liabilities, including direct, special, indirect, or consequential damages, are expressly disclaimed. Information provided in this publication is "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or freedom from infringement.

Special Acknowledgements

This document was adapted for MFSA from the **Nonprofit Coordinating Committee of New York, Inc.,** who in turn compiled the original version from a series of disaster planning and recovery seminars given for NPCC by the following individuals and/or reviewed by: American Red Cross of Greater New York; William Krouslis; Allen Breslow, Esq.; Joshua Peskay and Kim Snyder, Fund for the City of New York; Ken Liebman and Jack Stravidis, Frank Crystal & Company; John Burke, AIG; Bob Bender; Marcia Brown. Daniel Myers, compiler.

The original project was made possible with funding from Japan Relief Fund of The New York Community Trust.

Nonprofit Coordinating Committee of New York, Inc.
1350 Broadway, Suite 1801
New York, NY 10018
212.502.4191
www.npccny.org — info@npccny.org

The MFSA Risk Management Committee also dedicated many hours to this project throughout the course of several committee meetings and teleconferences.

II. Disaster Planning

Why You Should Have a Disaster Plan
Let's face it – on any given day, you have dozens of priorities vying for your attention. And disaster planning is probably low on your list. But a disruption to your business impacts your bottom line, and a prolonged disruption, such as a hurricane or major influenza outbreak which causes you to shut down completely for several days, could put you out of business entirely.

Whatever you choose to call it — disaster planning, crisis response, emergency preparedness, or business continuity — the goal is ultimately the same: to have effective plans and processes in place to get your business back up and running in the event of an interruption. What do we mean by "an interruption?" The problem could stem from something as localized as a computer crash or as widespread as a citywide blackout or flood. The impact of the interruption could range from an inconvenient loss of data to loss of revenues, or even loss of life. The difference between recovering from an interruption and closing the business for good may be attributed to having a disaster recovery plan that can be implemented quickly and that addresses your company's three biggest concerns: your employees, your customers and your assets.

What is a Disaster Recovery Plan?
A disaster recovery plan is a user's guide that documents, step by step, the actions you and your staff should take in response to an interruption. Planning cannot take place during a crisis – an effective disaster recovery plan must be documented well before an interruption occurs.

A well-crafted plan addresses all three phases of crisis response:

- *Emergency response* - immediate responses to an interruption in business (e.g., evacuation, employee and customer notification, securing the facility).

- *Disaster recovery* - steps taken to temporarily restore some functions so that some level of services can be offered (e.g., facility clean-up/inspection, data recovery, re-routing client jobs to other locations, access to emergency cash)

- *Business continuity* – restoration of most, if not all, business functions once the immediate threat is over (e.g., reopening the facility, replacing equipment, recalling furloughed employees)

Before you can write your disaster recovery plan, you must first do some research and planning. And once your plan is drafted, you must periodically review it with your team to ensure that everyone is clear on their role during an interruption. This is particularly important in operations with high employee turnover – in the event of an emergency, every employee should know what to do and where to go.

Unfortunately, when it comes to a disaster recovery plan one size ***does not*** fit all. This is not something that you can simply purchase as a form from a Website and fill in the blanks. You can definitely start with a template, since there are some common elements among plans (see “Resources” on page 8). But every plan will be different because every organization’s structure and circumstances are unique.

Possible Disasters/Disruptions

Part of writing a disaster plan is to think about all the possibilities for what can go wrong and make contingency plans that address those possibilities. However, you cannot reasonably plan for every scenario; it would take all of your time and the plan would never get done. So the goal is not to create a separate plan that addresses every risk, but to create one plan that addresses all risks, even the ones you cannot foresee. In other words, you do not create one plan for a tornado, one for a flood, and one for a blackout. You just need one plan that addresses all possible scenarios and can be adapted to address the unthinkable.

When creating your plan, a good first step is to consider how each of these events would affect your company. How would they impact your employees? Your customers? Your revenues? Your facility? Your systems and programs? Your suppliers and supply chain?

Natural Disasters/Disruptions

- Earthquakes
- Tornadoes
- Hurricanes
- Floods
- Fires

Man-Made Disasters/Disruptions

- Power/telecom/data outages
- Chemical spills/gas leaks
- Terrorist activities
- Influenza or other epidemics
- Transportation strikes
- Employee sabotage/workplace violence
- Theft/vandalism

Which of the events above are most likely to disrupt your company’s operations? Consider these risk factors in your discussions:

Historical: What types of emergencies have occurred in your business community, at your facility, or nearby? (e.g., fire, natural disasters, accidents, utility, etc.)

Geographic: What can happen as a result of your location? (e.g., proximity to flood-prone areas, hazardous material production, storage or use, major transportation routes, power plants, etc.)

Human Error: What emergencies might be caused by employees? Are employees trained to work safely? Do they know what to do in an emergency? Human errors can result from poor training and supervision, carelessness, misconduct, substance abuse, fatigue, etc.

Physical: What types of emergencies could result from the design or construction of the facility? Does the physical facility enhance safety? Consider the physical construction of the office, the facilities for storing combustibles or toxins, hazardous processes or byproducts, lighting, evacuation routes and exits, shelter areas, etc.

Once you've considered all possible disruptions and disasters, you should be able to categorize them into four scenarios:

1. **Local/minimal disruption:** a small flood that damages your files, a computer crash, or a fire contained to one office, a walkout by your evening crew.

2. **Local/significant disaster:** a fire or gas main explosion that destroys your facility, employee sabotage that destroys all business documentation, sudden death of a key company officer, vandalism/theft, or workplace violence that results in employee deaths.

3. **Wide-spread/temporary disruption:** an electrical outage or gas main explosion, seasonal influenza, transportation strike.

4. **Wide-spread/long-term disaster:** a hurricane, flood or tornado that displaces employees, a pandemic viral outbreak, or chemical spill that renders the area uninhabitable for an unknown amount of time.

Your disaster recovery plan should encompass each of these scenarios and should include activities to address your three most significant concerns:

- Employees
- Customers
- Revenues/Profitability

Assign a Team—You Cannot Create a Plan Alone

Who should create the disaster recovery plan?

The best way to ensure a comprehensive disaster recovery plan is to call upon representatives from all areas of your company to help create the plan. While small organizations may be able to get by with one person doing the work, larger organizations will have to enlist the assistance of others, particularly in coordinating various departments to provide needed information or context. For example, assign one team/person to complete the computer/technical portion, one person to complete the production operations portion, and another team to complete the personnel portion.

Depending on the size of your company and your employee culture, staff members may be motivated to take on this additional responsibility if they are given a special designation, such as “Emergency Response Team” and recognized for their efforts.

Who makes the decisions?

When creating the disaster recovery plan, be sure to include a clear statement regarding responsibilities, specifically, who has the authority to make short-term emergency decisions. It is vital that the “chain of command” be documented and understood by all.

For example, who will decide when to:

- Evacuate the building?
- Activate “liberal leave” due to weather conditions?
- Notify customers of business disruptions? Notify the media? Notify employees? Notify suppliers?
- Close the facility for several days?

Who is the “go-to” person and who is his/her back-up in case the primary person is unavailable? These people should include your leadership and could also be long-term employees or employees who are familiar with your disaster recovery plan and are most likely to be present in the event of an emergency.

Success Tips for Drafting a Disaster Recovery Plan

Keep it logical. Your plan needs specify which actions to take first, and who is responsible for that action. The logic and order of steps depends on the nature of your organization and its services as well as the type of disaster or interruption. The members of the Emergency Response Team will address this during the planning stages, particularly when analyzing the organization’s services and programs.

Keep it flexible. The plan has to be able to be implemented without the person or the team that created it being present to interpret or explain the details. And planning for the worst-case scenario, it should include some basic instructions for undertaking that action, in the event that the person responsible is incapacitated. If only a “techie” can implement your plan, it will most likely not be successful.

Keep it current. As things change in your organization—people come, people go, programs fold, programs start—the plan has to be updated to reflect these changes. The ideal candidate for maintaining and updating the plan is the person who headed the Emergency Response Team during the development of your plan, or someone who was involved with the process.

Keep it accessible. Your plan must be accessible from multiple locations -- keep in mind that during a disaster or an interruption, you can’t count on being able to access the facility to gather materials or dial in/log onto your network to access client files.

Battling Complacency
One obstacle to creating an effective disaster recovery plan is complacency. For example, management may not want to spend money on tech-related communication or back-up systems that may never get used. A SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis, which outlines various possible scenarios, including those where no resources are allocated and no plans in are in place, will go a long way to demonstrate the negative impact on your operations.

Resources: Sample Plans and Templates

- Department of Homeland Security: http://www.nsc.org/preparedness/documents/SampleBusinessEmergencyPlan.pdf
- Canadian Centre for Emergency Preparedness: http://www.ccep.ca/ccepbcp6.html
- Florida Business Disaster Survival Kit: www.fldisasterkit.com
- Institute for Business and Home Safety: www.ibhs.org/docs/OpenForBusiness.pdf
- Interactive Business Continuity plan generator from the Metropolitan Washington Council of Governments (free registration required): http://www.mwcog.org/security/security/continuity/intro.asp
- Your insurance broker
- Your city or state's Emergency Management Office

III. Creating Your Plan

Step One: Analyze Your Organization
As noted in the previous segment, disaster recovery plans are not "one size fits all." A good starting point for any disaster recovery plan is an in-depth discussion of your business. Begin by spending a few minutes with your Emergency Response Team in a discussion your organization's critical services and functions before diving into your planning.

Critical Services and Functions

- What does your company do? What services do you provide (be specific)?
- What department or staff team is responsible for each function? Which teams have multiple functions?
- Which functions and services are critical, and which are less so? What skills are required to perform the critical services and functions? Which equipment is required to perform the critical services and functions?
- Which executives are authorized to make key business decisions (hire/release employees, sign contracts, approve capital expenditures, speak to the media)?
- Who are your clients? Where are they located? How do you communicate with them?
- What services do you provide clients?
- What types of materials are required to produce your products? Where are they stored and how are they delivered to your location?

- Do you store supplies or materials on behalf of your customers? Where are those materials stored and how are they delivered to your location? Are they stored in multiple locations?
- How would an interruption impact your clients and the services you provide to them?
- How much time is needed to get back up and running? In other words, what is the acceptable level of downtime?
- Do you have a place for your staff or projects to go should your offices become unusable (e.g., through MFSA's Remote Facility Partnership Program – see Appendix C, page 20)

Once you've reviewed your organization's critical functions, the next logical step is to delve into key business processes for each of the following areas:

Information Storage

(Note: Recent legislation has led to new Federal and state guidelines for retaining business records.)

- What type of documents or data are critical to your business (e.g., personnel files, client profiles, project files, financial records, etc.)
- Where are crucial documents and backed up data files stored? In a fireproof, crush-proof, water tight safe?
- How frequently is data backed up? How long are documents retained? Are you retaining records in compliance with local and Federal guidelines? (see Appendix F, page 27)
- Are critical documents scanned or soft copies stored online, either in a password-protected portion of your company's intranet or in an offline server?

Intellectual Capital

- What is your organization's intellectual capital?
- How is intellectual capital archived?
- Who knows what about your services?
- Who knows what about your administrative infrastructure?
- Who would provide this information if those with the answers were gone?
- Does anyone else know or have access to these answers/this information?
- Is this information documented anywhere?

Computers & Technology

- Do you have an accurate and complete inventory of all computer and communication hardware and peripherals (printers, scanners, zip drives, servers, etc.) you would need to replace if your facility was damaged or destroyed?
- What additional hardware would you need to continue back office and administrative operations: phones, fax machines, pagers, walkie-talkies, etc?)
- Do you have an accurate and complete inventory of all business software and software licenses? Which programs are critical to restore your business operations?
- Do you have the ability to access these programs and files remotely, should your facility become inaccessible?

- Do you have an accurate and up-to-date diagram of your current computer configuration so your backup tapes can be restored and possibly transferred to a new facility?
- When was your vendor and supplier contact list (IT support, email, phone, company website, etc.) last updated? Where is it stored?
- Do you have a list of all passwords and logins needed to access remote servers and files? Is that list secured and stored in an offsite location?
- Can employees access telephone systems remotely? Can they access their data files remotely?

Your Physical Plant

- Do you have a site map at each facility that indicates shutoffs, valves, alarms, evacuation routes, etc., posted in all work areas?
- When the emergency contact list was last updated? Do you have a current and complete listing of all public service emergency contacts (both phone numbers and Website URLs)?
- Does the facility have a public address or alarm system? If not, do you have a notification system in place to contact each floor/area?

Resources:

- Appendix C – MSFA's Remote Facility Partnership Program (page 20)
- Appendix D - Financial Records Checklist (page 23)
- Appendix E- Record Retention Guidelines (page 27)
- Appendix F - Back up Your Data! (page 29)
- Appendix G - Facilities Management Checklist (page 31)

Step Two: Conduct a Risk Analysis

Risk analysis is the process of identifying credible threats that could cause an interruption to your business. Some risks can come from within, for example, in an onsite kitchen or hazardous cleaning chemicals storage room. Other risks come from external forces such as flood, fire, etc.

A thorough risk analysis should take into account an organization's physical surroundings, and include such concerns as security, emergency lighting in halls and stairways, fire escape routes and exits, storing of toxic chemicals, etc.

Do you have policies and procedures in place to address these situations?

- Evaluation (including procedures for employees and visitors who are disabled)
- Chemical spill
- Fire
- Workplace violence
- Natural gas leak

An analysis of risk should identify possible threats, as well as ways to reduce those threats. Some threats you can mitigate or avoid. And while you can't prevent a natural disaster, your Emergency Response Team can plan for what to do if such a catastrophe occurs.

Resources:

- National Fire Protection Association (codes and standards to minimize fire risk) www.nfpa.org
- Appendix H – Facilities Management Checklist (page 31)
- Appendix I – Insurance 101 (page 33)
- Your insurance broker
- Your local fire/police department
- Your local electric company and gas company
- Your local government's Office of Emergency Management

Step Three: Analyze the Potential Business Impact

A Business Impact Analysis determines how many days or weeks your business can survive without your regular stream of income before going out of business. When conducting your analysis, be sure to factor in the answers to these questions?

- How long will it take before the loss of income affects the delivery of your organization's services?
- How many payroll periods can you meet with no income?
- How many vendors must be paid in the short term in order to continue your business operations? Which ones?
- What is your cash reserve? Do you have additional assets that can be used to raise cash quickly?
- What is your RTO (Recovery Time Objective)? RTO is that point in time when a business expects to be back in operation. The RTO is at the discretion of the organization; it could be immediate or it could be protracted.
    - To determine your RTO, you have to examine each discrete, definable component of an organization — each department and its critical services that you want to resuscitate.
- How much cash would you need to purchase replacement equipment in order to resume operations in the event of an interruption?
    - This may be answered when you determine your RTO. If you require an immediate RTO, you will have to spend resources in order to achieve that. If your budget precludes spending resources, you have to adjust your RTO accordingly.
    - Your RTO will determine what resources you need to purchase or implement. It is important to recognize that if a quick recovery time objective is dictated, then resources will have to be spent in order to achieve that. For example, if it is imperative that your staff have electricity to power their computers and lights, then you will have to purchase a generator and you must allocate

resources for this to be accomplished. A quick RTO will cost more than a slower RTO.

- It is important to keep in mind that in an interruption there will always be a certain amount of downtime that you're going to have. In determining your RTO, another question to answer is what constitutes unacceptable downtime?

Step Four: Implement the Resources

Once you have:

- identified your critical services and functions
- determined your technology needs
- determined your Recovery Time Objective (RTO), and
- budgeted for the resources

You can purchase or plan for those resources needed to implement your plan.

Step Five: Draft and Test the Plan

With your research completed, the next step is to draft your plan. Take into account all the data collected during your research process and develop a plan to reflect your company and geographic location. Be sure to clearly identify roles and responsibilities, particularly in the areas of financial management, employee/media/customer communications, facilities inspections and data recovery.

It is absolutely vital that you test your plan to ensure that it works in practice and that the resources you've indicated in your plan actually exist. Testing of a plan can be done on the desktop by looking at your plan as written and speculating as to its worthiness and as an actual drill where you physically execute all the steps of the plan and set up operations elsewhere.

Whether you are conducting a "tabletop" exercise or a drill, the process is the same: Select a scenario and walk through the scenario step by step, ensuring that all significant elements are in place. This is a great opportunity to utilize your Emergency Response Team and recognize their efforts.

At the conclusion of the drill, you need to conduct a through assessment:

- **The Scenario:** Take a look at what happened, why it happened, and figure out how to ensure that it won't happen again. Could it have been prevented?
- **The Response:** What procedures worked well? What systems did not function well? How well did the team communicate during the drill? How well did the team communicate with employees, media, customers, etc., during the drill?
- **The Recovery:** How long did it take to resume normal business operations? How much revenue was lost during the disruption? Were there employee injuries or loss of life? What additional procedures should you implement as a result of that interruption?

Maintain and Update the Plan

Keep the plan current. When you buy new equipment, document it. As staff come and go, change the plan to reflect new responsibilities and make sure new employees know and understand their role in the plan.

Resources:

Appendix A – Emergency Planning Checklist (page 15)
Appendix B – Online Resources (page 18)
Appendix J – Crisis Communication Basics (page 35)

Step Six: Train Your Employees

The best plan in the world is doomed to failure if your employees don't know what to do during an interruption. Once your plan has been tested and fine-tuned, take this opportunity to educate your employees on the new procedures. Make disaster recovery training part of your employee orientation and set a schedule for frequent reminders so safety and disaster recovery become second nature to your staff.

A good employee awareness program should always include reminders about:

- Individual roles and responsibilities;
- Information about threats, hazards, and protective actions;
- Notification, warning and communications procedures;
- Processes for locating family members;
- Emergency response procedures;
- Evacuation, shelter, and accountability procedures;
- Location and use of common emergency equipment; and
- Emergency shutdown procedures.

Build emergency preparedness into the culture of the organization. Orientation sessions for new employees should include an overview of the contents and a copy of the preparedness manual and shift change meetings and training sessions should periodically review key components of your disaster recovery plan.

IV. Appendix: Additional Resources

Appendix A - Emergency Planning Checklist

Refer to this checklist frequently while developing your disaster recovery plan to ensure your Emergency Response Team has addressed the most critical issues.

PLANNING TEAM	**YES**	**NO**
Planning Team established?	□	□
Planning Team schedule established?	□	□
Budget developed?	□	□
INTERNAL PLANS AND POLICIES REVIEW		
Evacuation Plan	□	□
Fire Protection Plan	□	□
Safety and Health Program	□	□
Security Procedures	□	□
Insurance Programs	□	□
Employee Manual	□	□
CODES AND REGULATIONS REVIEW		
Fire Codes	□	□
Electrical Codes	□	□
OSHA Regulations	□	□
CRITICAL SERVICES AND OPERATIONS REVIEW		
Services provided by your company identified?	□	□
Operations vital to the continued functioning of the facility?	□	□
Equipment vital to the continued functioning of the facility?	□	□
Personnel vital to the continued functioning of the facility?	□	□
Services provided by vendors identified?	□	□
INTERNAL RESOURCES AND CAPABILITIES REVIEW		
Personnel		
CPR Training	□	□
First Aid Training	□	□
Equipment		
Fire Protection	□	□
Communications	□	□
First Aid Supplies	□	□
Emergency Power	□	□
Backup Systems (Arranged with other facilities)		
Payroll	□	□
Communications	□	□
Customer Services	□	□
Computer Support	□	□

EXTERNAL RESOURCES REVIEW

Emergency Management Office	□	□
Fire Department	□	□
Police Department	□	□
Emergency Medical Services	□	□
Telephone Companies	□	□
Electrical and Other Utilities	□	□
Insurance Policy Review with Broker	□	□

PLAN DEVELOPMENT

Plan Purpose	□	□
Responsibilities of key personnel	□	□
The types of emergencies that could occur	□	□
Where response operations will be managed	□	□

EMERGENCY MANAGEMENT ELEMENTS IN PLACE

Direction and Control	□	□
Communications	□	□
Life Safety	□	□
Property Protection	□	□
Community Outreach	□	□
Recovery and Restoration	□	□

EMERGENCY RESPONSE PROCEDURES ADDRESSED

Assessing the situation	□	□
Protecting employees, customers, visitors, equipment, vital records, other assets	□	□
Getting the business back up and running	□	□

PROCEDURES FOR BOMB THREATS ADDRESSED

Warning employees and customers	□	□
Communicating with personnel and community responders	□	□
Conducting an evacuation and account for all persons in the facility	□	□
Shutting down operations	□	□
Protecting vital records	□	□
Restoring operations	□	□

SUPPORT DOCUMENTS AVAILABLE

Emergency Call Lists – Responsibilities and telephone numbers	□	□
Employee Lists – Employee home and cell phone numbers	□	□
Resource Lists – Equipment and supplies that could be needed in an emergency	□	□

DEVELOPMENT PROCESS

Task list identifying persons, tasks and timetables	□	□
Needs of disabled persons and non-English speaking personnel	□	□
Training schedule for employees established	□	□

PLAN DISTRIBUTION

Copies distributed to employees	□	□
Current date and revision number on plan	□	□

PLAN IMPLEMENTATION

All personnel trained in procedures	□	□
Orientation and Education Sessions	□	□
Walk Through Drills	□	□
Evacuation Drills	□	□
Plan tested to assure that employees know what to do	□	□

EMPLOYEE TRAINING ADDRESSES:

Individual roles and responsibilities	□	□
Information about threats, hazards, and protective actions	□	□
Notification, warning and communication procedures	□	□
Means for locating family members in an emergency	□	□
Emergency response procedures	□	□
Evacuation, shelter and accountability procedures	□	□
Location and use of common emergency equipment	□	□

PLAN EVALUATION AND MODIFICATION

A formal audit of the plan conducted at least once a year	□	□
Does the plan reflect lessons learned from drills and actual events?	□	□
Are photographs and other records of facility assets up to date?	□	□
Are the names, titles and telephone numbers in the plan current?	□	□

Appendix B: Online Resources

Sample Plan Templates

- Department of Homeland Security: http://www.nsc.org/preparedness/documents/SampleBusinessEmergencyPlan.pdf
- Canadian Centre for Emergency Preparedness: http://www.ccep.ca/ccepbcp6.html
- Florida Business Disaster Survival Kit: www.fldisasterkit.com
- Institute for Business and Home Safety: www.ibhs.org/docs/OpenForBusiness.pdf
- Interactive Business Continuity plan generator from the Metropolitan Washington Council of Governments (free registration required): http://www.mwcog.org/security/security/continuity/intro.asp

Non-Profit and Professional Associations

Disaster Planning and Relief

American Red Cross: www.redcross.org
U.S. Chamber of Commerce: www.uschamber.com
Nonprofit Risk Management Center: www.nonprofitrisk.org
Institute for Business and Home Safety: www.ibhs.org
National Emergency Management Association: www.nemaweb.org
National Fire Protection Association: www.firewise.org
Public Entity Risk Institute: www.riskinstitute.org
Association of Contingency Planners: www.acp-international.com
Disaster Recovery Institute International: www.drii.org
Disaster Emergency Response Association International: www.disasters.org
Global Partnership for Preparedness: www.globalpreparedness.org
The Business Continuity Institute: www.thebci.org

Crisis Communications

Public Relations Society of America: www.prsa.org
International Association of Business Communicators: www.iabc.com

Technology

American Power Conversion: www.apcc.com

NPower: www.npower.org *Preparation, Planning & Peace of Mind: Top Ten Business Continuity & Disaster Planning Tips for Nonprofits* available online at http://tadev.npower.org/tools/resources.asp

Non-Profit Coordinating Committee of New York: www.npccny-whodoeswhat.org database of nonprofit technical assistance and information providers, from board governance to insurance, financial management to technology

Facilities Management and Insurance

International Facility Management Association: http://www.ifma.org/
Facilities Management "FMLink" (requires free registration): http://www.fmlink.com/
MFSA Insurance Program: http://www.mapinsurance.com/content.asp?CID=317

Federal Agencies and Resources

Centers for Disease Control and Prevention: www.cdc.gov
Federal Emergency Management Agency: www.fema.gov
IRS: www.irs.gov
Occupational Safety and Health Administration: www.osha.gov
U.S. Department of Homeland Security: www.ready.gov
United States Small Business Administration: http://www.sba.gov/idc/groups/public/documents/sba_homepage/serv_da_disastr_revcovery_plan.pdf

State Government Agencies and Resources

New York State Emergency Management Office: http://www.semo.state.ny.us/index.cfm
State of Arizona Emergency Management Recovery Office: http://www.dem.state.az.us/operations/guidebook/index.htm
State of California Emergency Preparedness Office: http://www.dhs.ca.gov/ps/ddwem/environmental/epo/epoindex.htm
State of Florida Business Disaster Survival Kit: www.fldisasterkit.com

Appendix C – MFSA's Remote Facility Partnership Program

The MFSA-sponsored Remote Facility Partnership Program (RFPP) is a voluntary arrangement facilitated by the association to help provide its members an opportunity to establish informal partnerships to maintain operations in times of need. If your organization has an equipment breakdown, power failure or simply needs assistance with volume or deadlines, the program may be beneficial to your organization.

In order to create optimal partners, certain compatibility needs to be established between the partners. The compatibility of equipment, data processing software and distribution should be known to all parties involved, prior to any job sharing begins, which should reduce any difficult situation with a partnered job.

There are many details that would need to be defined. The objective would **not** be a business alliance for financial growth, but an MFSA-sponsored program that provides a safety net in times of need.

One scenario example would be to consider your partner's operating system – Printstream, Mail-Shop, ProMail, etc. If your organization uses Printstream as its operating software, GMC as your main data processing platform, and need someone with a Lake System 100% verification (or equivalent) capability, you will want to know that prior to any partnership is arranged.

Participating in the RFPP
First, take a few minutes to complete this Operations Profile of your business:

1. Operating System: Printstream, Mail-Shop, Pro-Mail, Custom built, ________________, ________________,
   - Data Processing Laser-print Platforms: GMC, ______________, __________________, ________________
   - Data Processing List Hygiene Platforms: BCC, ___________, ______________, _________________

2. Laser Printing: Cut Sheet: simplex only, simplex & duplex, 1 color (black) only, spot color, 4 color, __________,
   - Continuous Form: simplex only, simplex & duplex, ____________, _____________
   - Special: pressure sensitive label capability, direct impact printing capability, ____________________,

3. Intelligent Inserters: Gunther model __________, B&H model _____________,
   - Read 2-D barcodes in-line, need 100% verification in-line, _______________, _______________
   - Standard Inserting needs: up to 6 inserts, up to 8 inserts, up to 10 inserts, up to 20 inserts, _____________,
     1. Meter in-line, stamp in-line, friction feed capability, ____________,

    2. Only #10 needed, up to 6x9 env, #11 env needed, up to 9x12 env, _____________, __________

4. Ink jet needs: 1” printhead, 2 ¼” printhead, 4” printhead, _______________, _______________
    - Spot color, top & bottom in-line capability, ____________________, ________________
    - 150 dpi, 300 dpi, 600dpi, _________________, ________________

5. Polywrapping: small run poly capability, large run poly capability, _______________, ________________

6. Ink jet address in-line, Cheshire label on-poly in-line, ________________, _________________

Next, review the list of participants and, based upon location and capabilities, reach out and establish your own RFFP company. A complete listing of all participants to date, including contact information and company service capabilities can be found in the Members Only section of www.mfsanet.org.

Appendix D - Personnel Policies

Revise Your Payroll Policies to Reflect Disruptions to the Business

Update your personnel manual to reflect new realities such as emergency closing policies, workplace safety, telecommuting, etc. You should document how to handle a number of scenarios such as:

- Paying non-exempt employees when the facility is closed.
- How to handle an employee absence caused by mandatory road closures, severe weather, etc.
- What to do if an employee comes to work and finds the office closed.

Note that some states mandate how employees must be compensated during natural disasters and other crises; your policies should always be in compliance with local and state employment laws.

Workers Compensation

Workers' compensation is a no-fault system for accidents that occur within the scope of the job. Disability coverage is for off-the-job accidents. Workers' comp would include injuries that arise during an emergency at work. An injury at home for a worker who is telecommuting should be covered by workers' compensation. Stress (a mental injury without physical injury) would also be covered by workers' compensation.

An organization's employee handbook should include a statement requiring all employees to immediately report all and any injuries to management.

Telecommuting

Telecommuting has to be planned, it can't be haphazardly implemented, and personnel policies must address the situation. It is easier for an executive or other exempt employee to telecommute. You must determine how to track the time of an hourly, non-exempt employee should a telecommuting option be offered and consider how these employees will be supervised remotely.

Notify your workers' compensation carrier that there are employees who are working from home and the days they are doing so. There is no home inspection requirement, since OSHA has come out with a ruling saying so. A workers' compensation claim for a telecommuter may come down to the word "regularly." If they work on Fridays at home, workers' compensation may not cover an injury that occurred on a Wednesday.

Accommodating Employees' Distress

In the event of a catastrophe, you may need to address scheduling problems as well as employees who are afraid to come to work. Telecommuting and split schedules may be some of the ways to help alleviate these issues. Don't dismiss your employees' concerns; some companies have had success treating these issues the same way they would a personal crisis. The American Red Cross (www.redcross.org) offers counseling and support services that might benefit your employees.

Appendix E – Financial Records Checklist

Payroll and Facility Information

Know where your organization’s information is stored so you could pack up and resume operations from another location.

	onsite& where	offsite & where
Current and previous audited financial statements	□ ________	□ ________
Financial Statements and 1099s	□ ________	□ ________
Blank Checks	□ ________	□ ________
Computer passwords	□ ________	□ ________
Employee Payroll Records	□ ________	□ ________
Client Records	□ ________	□ ________
Office Lease (for renters)	□ ________	□ ________
Building Deed (for owners)	□ ________	□ ________
Other Vital Records	□ ________	□ ________

Payroll Information:

Company Name ________________________________

Account Number ________________________________

Payroll Rep ________________________________

Telephone & email ________________________________

Insurance

General Liability / Commercial Umbrella

Company / Underwriter: __________________________

Policy Number: __________________________

Representative, telephone & email: __________________________

Broker, telephone & email: __________________________

Key Man Liability

Company / Underwriter: ___________________________

Policy Number: ___________________________

Representative, telephone & email: ___________________________

Broker, telephone & email: ___________________________

Health Insurance Company

Company / Underwriter: ___________________________

Policy Number: ___________________________

Representative, telephone & email: ___________________________

Broker, telephone & email: ___________________________

Unemployment Insurance

Company / Underwriter: ___________________________

Policy Number: ___________________________

Representative, telephone & email: ___________________________

Broker, telephone & email: ___________________________

Workers’ Compensation

Company / Underwriter: ___________________________

Policy Number: ___________________________

Representative, telephone & email: ___________________________

Broker, telephone & email: ___________________________

Disability Insurance (short-term)

Company / Underwriter: ___________________________

Policy Number: ___________________________

Representative, telephone & email: ___________________________

Broker, telephone & email: ___________________________

Disability Insurance (long-term)

Company / Underwriter: ___________________________

Policy Number: ___________________________

Representative, telephone & email: ___________________________

Broker, telephone & email: ___________________________

Life Insurance

Company / Underwriter: ___________________________

Policy Number: ___________________________

Representative, telephone & email: ___________________________

Broker, telephone & email: ___________________________

Dental

Company / Underwriter: ___________________________

Policy Number: ___________________________

Representative, telephone & email: ___________________________

Broker, telephone & email: ___________________________

Long Term Care

Company / Underwriter: ___________________________

Policy Number: ___________________________

Representative, telephone & email: ___________________________

Broker, telephone & email: ___________________________

Retirement Plan

Company / Underwriter: ___________________________

Policy Number: ___________________________

Representative, telephone & email: ___________________________

Broker, telephone & email: ___________________________

Financial Information

Bank Name(s): ______________________

Account Numbers: ______________________

Branch Representative: ______________________

Telephone, fax, email: ______________________

Investment

Financial Planner / Broker Company: ______________________

Rep name: ______________________

Telephone, email: ______________________

Who is authorized to make bank transfers? ___________________________________

Are there alternatives? ____

Who is authorized to sign checks? ____

Are there alternatives? ____

Appendix F - Record Retention Guidelines

Here are some general guidelines for retaining business documents and records. Please note that these requirements vary from state to state, so be sure to check with your locality for specifics.

Type of Document	**How Long to Keep** (Minimum)
Articles of Incorporation, amendments, bylaws	permanently
Certificate of incorporation and corporate records to the state	permanently
Tax returns	permanently
Work sheets and related backup documents for tax returns	7 years
Minutes from board or shareholder meetings	permanently
Annual corporate reports	permanently
Property records	permanently
Contracts and leases in effect	permanently
Insurance policies (including expired policies)	permanently
Insurance letters/correspondence	permanently
Audit reports of CPAs and financial statements	permanently
Employment applications (for current employees)	permanently
Bank statements and reconciliations	7 years
Canceled checks for standard transactions	7 years
Invoices from vendors	7 years
W-2 or 1099 forms	7 years
Housing allowance forms	7 years
Business correspondence	3 years
Employee personnel records (after termination)	3 years

Record Retention Tips

- When developing a record retention policy, it is important to think about where those files will be kept, how secure those files will be, and the conditions under which files will need to be stored (heat and particularly dampness can be very destructive to files).

- Some of the reasons to keep files and records include legal requirements, potential relevance in future litigation, and the needs of the organization, as well as historic importance. It goes without saying that should there be threatened litigation or an investigation on a certain subject matter, particular care should be given that no file or document relating to that matter is destroyed.

- Tax returns and governmental reports affecting tax liability should be kept permanently. However, most backup records, such as receipts documenting income deductions need only be kept for seven years. The Internal Revenue Service (www.irs.org) calls for a six-year statute of limitations. The IRS has three years from the date of when the income tax return is filed to question or audit it. If the IRS can prove an omission of at least 25%of income, the time period doubles to six years. Therefore, the seven-year period gives a one-year cushion beyond that time limit.

- Of particular importance is the retention of insurance policies and related documents. From time to time, lawsuits are brought which reach back many years. Therefore, it is important to determine the policy in effect at the time that a claim arose. Should those policies be missing, they can often be recreated by contacting your broker or insurance company to establish coverage.

Appendix G - Back Up Your Data!

Whether your office has one computer or hundreds, once data is lost, it is virtually impossible to recover. Without back-up you may lose all business records forever.

Analyze your data backup routine
Create backups, verify the data, and take your back-ups off-site. This process can be as simple as having someone regularly taking the backup home or it could be high-level, clustering or mirroring the server at an off-site location. The latter, however, is an expensive way to ensure data security.

Do a backup, test for validity, and restore
If you're going to bother doing backups, you need to test to ensure that you can actually restore the data. Decide how frequently you will test the backup-up system. Some recommend testing restoration every six months, by bringing the entire system down and then restoring it to see that everything is working properly.

Be sure that your backups include all important and pertinent files
For example, are all staff email address books being backed up? Another option may be to synchronize address books with PDAs. Or encourage employees to make a hard copy of their contacts. Those who use a Rolodex should make a copy and take offsite.

Determine what kind of archival system of the backup media you will maintain
For example, one tape used repeatedly will not provide an archive. You may need to establish a rotation system to get to, at a minimum, one-month old data. Always keep a copy off-site as a theft of the only existing backup tape won't help with data restoration. If an organization needs to maintain a history of data, you have to deal with constantly changing media. So, if you're storing data on a yearly basis, you'll need to move it to new media.

Other Data Options

- Make your databases Web-based. For example, use an ASP (application service provider) or house your database offsite on an encrypted server so that nothing is stored in-house.
- Store essential data on portable computers. However, this raises other security concerns such as theft, damage, or lost computers. It also raises issues of security of documents and data that you don't want others to access. And, if documents and data stored on the laptops are accessed and altered regularly they will still require some form of backup.
- Purchase an external, easily portable way to backup data and take offsite, for example writing to DVDs, an iPod, thumb drive or other self powered USB device.
- Investigate a co-location server. A co-location server is where an organization purchases and installs a server in another location. The data from the main office is then mirrored to the co-location site. There are numerous companies providing this service.

Power and Servers
A UPS (uninterrupted power supply, also known as a battery backup system) will supply a limited amount of power in the event of an electrical outage. Ideally, servers power switches, and routers have power backups so that in the event of power loss, you are able to shut down your network without causing damage to the server and other equipment.

American Power Conversion (www.apcc.com) has a resource to help determine what battery backup system is best suited to your equipment configurations and desires. It's not necessarily a good idea to have monitors plugged into UPS devices because they will drain the power quickly.

- Firewall drives are imperative for network systems that are always on. Without a firewall, you are opening up your system to hackers and others who can hijack your site without permission.
- If you have a T1 line, and all telephones, internet, and email services go through this line, and it goes down, you'll be dark. If appropriate, make contingencies for this such as setting up back-up landlines for clients and/or staff use.

Set up a free email account (HotMail, Yahoo, GMail, etc.) for emergency use. Document this and share this email address with key personnel.

Appendix H - Facilities Management Checklist

Document the Building

Create a site map for each facility or location that indicates the location of each of the following:

- Utility shutoffs
- Water hydrants
- Water main valves
- Water lines
- Gas main valves
- Gas lines
- Electrical cutoffs
- Electrical substations
- Storm drains
- Sewer lines
- Floor plans
- Alarm and sounders
- Fire extinguishers
- Fire suppression systems
- Exits
- Stairways
- Designated escape routes
- Restricted areas
- Hazardous material storage (cleaning supplies and chemicals)
- High-value items

Know your Emergency Contacts

Create a list of emergency contacts, including: local police precinct, fire department, gas, power and other utility companies, poison control, electrician, plumber, insurance adjuster, architect, building managers, etc.

These documents should be accessible to the appropriate personnel (office manager, building superintendent, etc.) and available to them both on and off-site.

Examine Your Plant for Safety and Security Weaknesses

The Occupational Safety and Health Administration offers helpful tips for facility safety planning on the OSHA site (www.osha.org). Here are some sample questions:

- Are the batteries for emergency lighting checked regularly?
- Do stair treads have reflective glow-in-the-dark strips to aid in dark exits?
- Are foot traffic zones clearly marked?
- Do electric door/key pad locks have a manual bypass cylinder lock?
- Are fire extinguishers easily accessible? Are they checked regularly? Do people know how to use them?

- Are dangerous/hazardous/flammable substances stored properly? Are employees trained on how to use them?
- Are first aid stations stocked and readily available? Are any employees trained in first aid?
- Are emergency shut-off switches on machinery clearly marked?
- Do you regularly test your emergency exit routes?
- Are emergency exit routes posted on the back of restroom doors?
- Is there a system in place to account for employees following an evacuation?

Have Emergency Supplies on Hand
Make contingencies should staff be required to stay inside (i.e., a dirty bomb or a hurricane). Stock a secured room with sufficient water, food, first aid supplies, flashlights, radios, batteries, extra clothing and a variety of communication devices (cell phones, walkie-talkies, landline phones, PDAs, etc.) to accommodate your staff for at least 24 hours.

Identify Alternative Vendors
Ensure that your critical suppliers of services and supplies will be available to you when you need them. Have, at minimum, two or three sources for your critical materials or services. If one is local, an alternate should be elsewhere in the state, region or nation.

Your vendors must have their own disaster recovery and business continuity plans, and responding to your needs must be a part of their plans. Ask to see documentation of this response commitment.

Appendix I – Insurance 101

Most businesses, whether they rent or own their facility, have property and general liability insurance. Landlords will generally require the renter to carry general liability insurance for both the tenant and the landlord for claims arising out of the premises described in the policy. Property insurance covers “first party” losses, such as damage to or loss of personal property or equipment, etc. Liability insurance covers claims from “third parties”, such as a visitor who injured while at your facility.

As part of your disaster recovery plan development, you should:

- **Review your current coverage** to ascertain whether it is adequate in the event of either a catastrophe or an interruption in business activities.
- **Review your workers’ compensation policy** to ensure that all personnel, including volunteers, are covered.
- **Review all policies for exclusions**. For example, what would happen if you were denied access to your premises by a civil authority? (Check your property coverage to see if this is included).
- **Document your facility.** Do you have photographs of the physical plant and machinery? Are photographs and other records of facility assets up-to-date? Are they stored in a safe place?
- **Consider your property for possible losses and damage:**
  - What is the cost to replace your equipment?
  - What would it cost to set up a temporary facility from which to operate?
  - What is the cost to repair the facility and the equipment?

Beyond property and liability insurance, and with regard to disaster planning, there are other types of insurance that an organization may want to investigate: Business Interruption, Extra Expense and Terrorism:

- **Business Interruption** pays for your loss of net profits plus expenses that continue for a period of time;
- **Extra Expense** will pay expenses above your normal expenses so that you may continue to operate. For example, if you had to move and pay increased rent, extra expense insurance would pay the additional rent, assuming you purchased enough insurance to cover the additional rent.
- **Terrorism** insurance used to be included in all forms of insurance. However, after 9/11 things changed; and this is no longer the case. Depending on state law, underwriters may not include terrorism insurance. Should you decide to purchase terrorism insurance, be sure to read the exclusions and endorsements. If you are not sure what is covered and what is not, consult your agent or broker.

Talk to your insurance broker or carrier to see if they can help with your planning. It’s in their best interest to see that your organization is prepared (to help mitigate their losses) and many are willing to help.

Minimize Risks

- One component in purchasing insurance coverage most cost-effectively involves analyzing and avoiding risk. For example, if you have plate glass windows, replace them with safety glass; if you have worn and torn carpeting, replace it; install self-locking safety exit doors, etc.
- When shopping for new coverage, ask your agent or broker for currently-valued loss experience from the insurance carriers for the past five years. You should actually check this every year, as you may find claims that are in excess of what you think they should have been and/or you may find claims that are charged to your policy that belong to another insured.

How Much Insurance?

To determine how much insurance to purchase, you must first determine the replacement value of the assets you want to insure.

- Many insurance policies cover only the Actual Cash Value (depreciated value) of your property.
- If you are going to replace this property, you will probably want to insure it for what it will cost to replace it presently.
- Ask your agent or broker to tell you the difference in cost between Actual Cash Value and Replacement Value coverage. Then determine how you want to insure it
- Look at your assets/cash reserve to see how much you are “willing” to spend on insurance, after you know what the premiums will be.

Information on the MFSA Insurance Program can be found at http://www.mapinsurance.com/content.asp?CID=317.

Appendix J – Crisis Communications Basics

Communicate with Your Employees

- Designate a leader or key staff member who will coordinate employee notifications and ongoing communications. Make sure that person is included in the decision-making process for closures, evacuations, etc., and is familiar with the overall disaster recovery plan.
- Create a system to communicate with your staff, especially if your company has multiple facilities or locations. This system can be as low-tech as an index card listing names and contact numbers that is carried at all times, or a high-tech solution such as text messages or voice mail alerts.
- Keep accurate and comprehensive contact information on all employees, including home phone number, cell phone or pager, number, personal email address, and phone number for the employee’s designated emergency contact person.
- Develop a telephone chain (or telephone tree) that defines who calls whom, making sure that the work of contacting every employee does not fall to a single person. Conduct an unannounced test of the telephone tree about once per quarter to ensure you can get in touch with everyone.
- Make back-up arrangements in the event of a phone outage at your facility. You may want to establish an incoming phone number that employees can call in the event of an emergency to find out whether and where to report for work. As an alternative, you can arrange for an answering service with either a message or a live person with info for staff on what to do and where to report.
- Remember to use your telephone chain to notify your employees when you are ready to resume operations.

Communicate with the Media

- Designate one person as your company spokesperson and make sure everyone in the company knows who that is. He/she should be the only person answering media questions or granting interviews and should be informed immediately as events unfold.
- Create a basic “fact sheet” about your company (name, address, when founded, type of business, number of employees, etc.) that can be distributed to the media.
- Basic interview rules:
    - Stick to the known facts; don’t speculate or give unnecessary details.
    - Show empathy and concern for the people impacted by the crisis.
    - Acknowledge that you don’t know the answer to something; never answer with, “No comment.”
    - Keep your answers short and to the point; don’t ramble or go off on a tangent.
    - Provide as much information as possible about the actions taken to ensure employee safety, respond to the crisis and resume operations.
    - Let the media know when you expect to have more information (within the next three hours, the next business day, etc.)
    - Never release specifics about injured staff members before their families have been notified.

- In most cases, a business disruption is a local news story, limited to a one or two-day news "cycle", and that media can be managed by your company spokesperson. But in the event that your company's disaster expands beyond two-day's coverage, or turns into a national story, you should identify in advance one to three local PR agencies to turn to for assistance on short notice. A good resource is your local Chamber of Commerce or your local chapter of the Public Relations Society of America (www.prsa.org).

Communicate with Your Customers and Suppliers

- Have contact information for all current clients and suppliers – office/cell phone, email, and pager – and have a plan to notify them in the event of a business interruption.
- Although it is ideal to designate one person to handle all client notifications, that may not be possible, given the size of your company. If you must rely on staff members to contact customers, make sure they know when to reach out to clients and what to say. Brief them in the basic interview rules outlined above provide our staff with a simple "script" or statement for customer notification to insure the information is accurate and free of speculation.
- Be sure to let customers know that you will follow up with them once you have resumed operations.