HAZARD PREPAREDNESS AND BUSINESS CONTINUITY PLANS

Prepare and Protect Your Business

The number of declared major disasters has doubled since the 1990s. Because of this, preparedness is a critical issue. Every situation is unique, but organizations can better withstand a difficult time if owners and decision-makers carefully plan and put procedures in place for likely types of emergencies. How quickly your business can recover, and how well it can continue to operate under suboptimal conditions, depends on the planning done today. A commitment to planning today will help support employees, customers, and the community. It also protects your business and gives you better chance of survival. Every business should have a hazard preparedness and business continuity plan. Get ready now!

Topics the Plan Should Cover

Mitigation
Efforts attempted to prevent hazards or emergencies from developing, or limiting the effects when they occur. The mitigation phase focuses on long-term measures for reducing or eliminating risk.

Preparedness
Continued cycle of planning, organizing, training, equipping, and exercising, to help respond and recover from disasters or emergencies.

Response
Mobilization of the necessary services to respond to needs.

Recovery
Restoring the affected area or persons to the previous state. Recovery efforts focus on replenishing and repairing essential supplies and infrastructure, as well as on restoring the well-being of persons affected.

On the following page you will find an example of what a resource management and recovery plan should cover. To do a basic disaster preparedness plan, you would develop a document covering the areas shown for each of the disasters or hazards most likely to affect your business. Think about:

- Geological hazards: earthquakes, volcanos, sinkholes, mudslides, tsunamis
- Meteorological hazards: tornados, hurricanes, blizzards, lightning strikes and the wildfires they cause, hailstorms, floods
- Biological hazards: epidemics, toxins
- Technology events: system crashes, data and communication losses
- Human-caused events: accidents like plane and vehicle crashes, structural failures, and injuries to key people intentional acts like terrorism, arson, and workplace violence
- Hybrid events like failure of the global financial system, riots, or declarations of martial law

Disaster Type ______________________________

	PREPARATION	RESPONSE	RECOVERY	MITIGATION
People and Training • Key positions • Training and preparation				
Facilities • Required facilities • Backup facilities • Features/outfitting • Contingency plan for temporarily operating without adequate facilities				
Systems and Equipment • Required systems and equipment • Backup systems and equipment • Features/outfitting • Contingency plan for temporarily operating without key systems or equipment				
Materials and Supplies • Materials required for this disaster • Supplies required for this disaster • Acquisition plan • Storage plan • Contingency plan for temporarily operating without key materials and supplies				

Other Planning Essentials

Business Continuity Team and Outside Resources
To create your hazard preparedness and business continuity plan, you will need the help of the people who know the most about how things work in your business—and maybe some outside experts too. Organize a business continuity team and compile the plans you need to manage a business disruption. Also be sure to consult people outside your team who will have important information you will need when disaster strikes, especially:

- **Insurance experts.** Find out their procedure for investigating and paying claims. Be sure to probe what happens when the disaster is widespread and they must respond to many calls at once. You will want to understand how turnaround times are affected in these situations. You may also want to be sure you have the coverage you think you have. Explore whether you are covered for wind and flooding under certain conditions because these things are sometimes excluded from standard policies. Also make sure your limits are adequate and would actually replace your depreciated assets.
- **Government and regulatory officials, especially those responsible for essential services (power, water, wastewater treatment, etc.).** Each of these agencies must also have a disaster recovery plan. Learn about what is in them so you can adjust your own plans accordingly.
- **Suppliers.** Make a point to understand what your suppliers' disaster and recovery plans are as well. Whether the same disaster that affects you affects them may not matter if they can't get you what you need when you need it.

Information Technology
Information technology systems require hardware, software, data and connectivity. Without one component of the "system," the system may not run. Therefore, recovery strategies should be developed to anticipate the loss of one or more of the following system components:

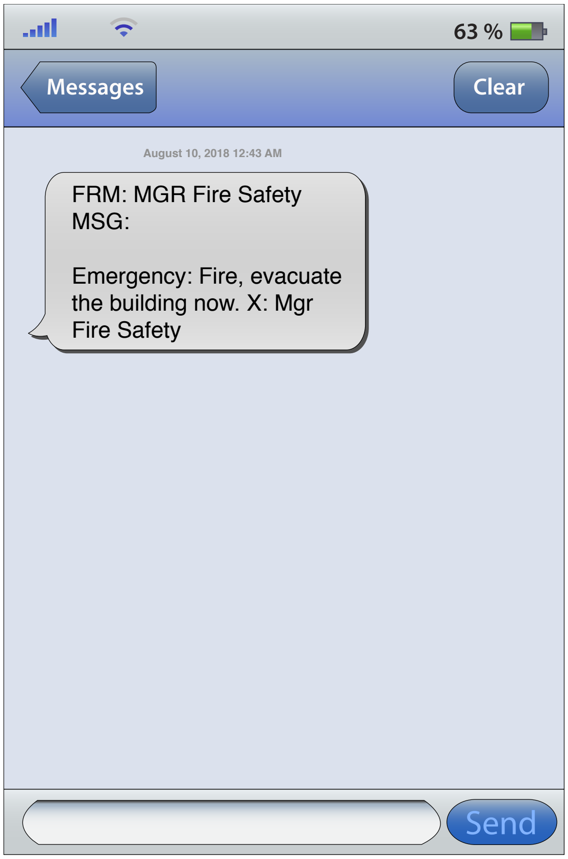
- Computer room environment (secure computer room with climate control, conditioned and backup power supply)
- Hardware (networks, servers, desktop and laptop computers, wireless devices
- Connectivity to a service provider (fiber, cable, wireless)
- Software applications
- Data and restoration

Crisis Communication Plan

Communication information should be complied in advance and immediately accessible during an incident or emergency. Include as much information as possible. The list should be updated regularly, secured, and available to authorized users only. Both electronic and hard copies should be kept in different locations. Possible contacts would be:

- Customers
- Suppliers
- Management
- Community resources
- Employees
- Victims/families
- Government and regulatory officials
- Media and press

Know which cellular carriers your employees use, and be prepared to send text messages (individual or group) via email networks. This is much faster than texting people individually via the little keyboard on your phone and may also save data charges. Each cellular carrier has a system for doing this. To send a text message via email, you must use an SMS to email gateway. Just substitute a 10-digit cell number for 'number' for each carrier below:



FRM: MGR Fire Safety
MSG:

Emergency: Fire, evacuate the building now. X: Mgr Fire Safety

- AT&T: number@txt.att.net
- Boost Mobile: number@myboostmobile.com
- C-Spire: number@cspire1.com
- Consumer Cellular: number@cingularme.com
- Cricket: number@mms.cricketwireless.net
- Google Fi (Project Fi): number@msg.fi.google.com
- Metro PCS: number@mymetropcs.com
- Page Plus: number@vtext.com
- Ptel: number@ptel.com
- Republic Wireless: number@text.republicwireless.com
- Sprint: number@messaging.sprintpcs.com or number@pm.sprint.com
- Suncom: number@tms.suncom.com
- T-Mobile: number@tmomail.net
- Ting: number@message.ting.com
- Tracfone: number@mmst5.tracfone.com
- U.S. Cellular: number@email.uscc.net
- Verizon: number@vtext.com (text-only), number@vzwpix (text + photo)
- Virgin Mobile: number@vmobl.com

Employee Assistance

Whether an emergency or disaster affects the local community or a remote location where employees may be working or traveling, you need to account for all employees as part of the emergency response plan. After accounting for all employees, assess the potential human impacts and determine appropriate assistance.

Providing assistance and support for employees should be part of a business' preparedness program. It should include communicating with employees and their families and providing support as appropriate. Employee information, typically compiled in a human resource information system, includes home addresses and telephone numbers. Consider asking for additional information including home email addresses and cellular telephone numbers (for text messaging/SMS). Also, request the name and contact information of a family member or friend who can be reached in an emergency. The confidentiality of this information should be protected and only be available to authorized users who are operating from their office, emergency operations center or alternate business facility.

Training

Training is essential to ensure that everyone knows what to do when there is an emergency or disruption of business operations. Everyone needs training to become familiar with protective actions and life safety. Review protective actions for life safety and conduct evacuation drills ("fire drills") as required by local regulations. Sheltering and lockdown drills should also be conducted. Even very small operations can be affected if a deranged individual appears on the scene and won't leave – especially if the person is brandishing some type of weapon or making threats. Employees should receive training to become familiar with safety, building security, information security and other loss prevention programs.

Members of emergency response, business continuity and crisis communications teams should be trained so they are familiar with their role and responsibilities as defined within the plans. Team leaders should receive a higher level of training, including incident command system training, so they can lead their teams. Review applicable regulations to determine training requirements. Records documenting the scope of training, participants, instructor and duration should be maintained.

Testing

You should conduct testing and exercises to evaluate the effectiveness of your preparedness program, make sure employees know what to do, and find any flaws or missing resources. There are many benefits to testing and exercises:

- Trained, confident personnel; clarified roles and responsibilities
- Reinforced knowledge of procedures, facilities, systems and equipment
- Improved individual performance as well as organizational coordination and communications
- Evaluated policies, plans, procedures and the knowledge and skills of team members
- Revealed weaknesses and resource gaps
- Compliance with local laws, codes and regulations
- Recognition of the emergency management and business continuity program