



BUSINESSLINK

We're here to help. Let's get started!

BUSINESS EMERGENCY

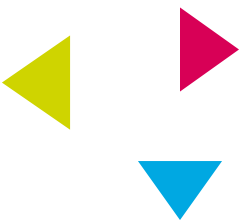
CONTINUITY PLAN



This Business Emergency Continuity Plan includes easy to use templates to help you address potential vulnerabilities that could cause disruption and business loss. The six critical business functions you must protect are: people; data; operations; inventory; equipment; and buildings. By working through each of these functions, you will be able to identify, prioritize and minimize risks for your business.



Be more prepared
and resilient!



UNDERSTAND YOUR SIX

CRITICAL BUSINESS FUNCTIONS

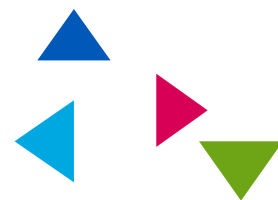


TABLE OF CONTENTS

Protect People	6	Protect Inventory	22
Take Action Now	7	Take Action Now	22
Templates	10	Template	23
1. Key Contact List	10	• Inventory Checklist	23
2. Key Emergency Contact List	11		
3. Key Customers List	12	Protect Equipment	24
4. Key Vendors/Suppliers List	13	Take Action Now	24
5. Key Visitors List	14	Template	25
6. Key Partners/Partnerships List	15	• Equipment List	25
7. Crisis Communications Plan	16		
8. Emergency Kit	17	Protect Buildings	26
		Take Action Now	26
Protect Data	18	Template	27
Take Action Now	18	• Understand Your Building 28	
Template	19	• Emergency Action Plan	29
• Emergency Business Data Kit	19		
		General Information	30
Protect Operations	20		
Take Action Now	20	List of Revisions	31
Template	21		
• Hazard/Risk Profile	21		

BUSINESS EMERGENCY CONTINUITY PLAN



Small businesses are highly vulnerable when it comes to emergencies and disasters especially if they have not taken the time to think about and plan for how they will handle potential business interruptions. Consequences can be dire in this respect. According to a report from the U.S. Federal Emergency Management Agency (FEMA), 40% of businesses do not reopen following a disaster. On top of that, another 25% fail within one year.

The good news is that it is not too late for you and your business to act now.

This **Business Emergency Continuity Plan** includes easy to use templates to help you address potential vulnerabilities with six of your critical business functions that could cause disruption and business loss.

These six business functions include: people; data; operations; inventory; equipment; and buildings. By working through each of the six business functions you will be able to identify, prioritize and minimize risks for your business.

Ideally you will use this Business Emergency Continuity Plan (BECP) to identify actions that you can take before during and after an emergency, to assist you in your business planning on an annual basis.

Make sure to update your plan on a regular basis, as information within each area will change over time.

Good luck in your efforts to be more prepared and resilient!

40%

40% of businesses do not reopen following a disaster. Another 25% fail within one year.



UNDERSTAND YOUR SIX CRITICAL BUSINESS FUNCTIONS

Every business, regardless of size or type, consists of critical business functions. While these business functions may vary from business to business, they will exist in each of them. Understanding what your critical

business functions are in advance will help you identify future vulnerabilities. **Protecting** these business functions is a priority.



PEOPLE

Employees
Customers
Vendors
Suppliers
Visitors
Partners

PROTECT PEOPLE

YOUR RELATIONSHIPS - BRAND & COMMUNICATION

The people your company interacts with are one of the most important yet often overlooked assets when planning for a disaster. How you communicate with them when disaster strikes will affect your recovery and the perception of your brand.

The first step in preparing to communicate effectively and protect your brand is to ensure that you have working lists at hand that will help you to quickly engage all the people who matter in a time of crisis. Your lists should include not just those who are internal to your firm but also all those who are external but needed for your recovery.

Internal Groups:

You cannot run your business without your employees, current customers, vendors/suppliers, partners in purchasing and marketing, landlords and other key internal people critical to the success of your business. These are your buyers, suppliers, partners and the staff who keep your operation running.

External Groups:

These are people that support your existing business operations, are affected by your brand or reputation, or who could become part of your internal operations in the future. Includes potential customers, the public and government/regulatory agencies.

✓ Potential Customers:

- Often business owners focus on existing customers during a disaster, which is important; however new customers can also be an opportunity. For example, after a disaster some people will be actively seeking a new supplier for their own needs or be motivated to shop local to help their community.
- Are there new people or customers in your community now that can use your product or

service? How can you market to them? Can they pass on information to others about your business?

✓ General Public:

- These are also potential customers for you. Do they know about you? Can they tell others about you?
- Newspapers, radio stations, online news gathering sites, etc. will be seeking stories of those affected by the disaster – use it as an opportunity to further your brand.

✓ Business Organizations:

In an emergency that affects many businesses there will be assistance available, but they will need to know you need help.

- Chamber of Commerce business outreach programs
- Local economic development groups
- Business area development organizations
- Local, regional and federal business assistance programs
- Educational institutions that may offer student assistance for recovery

✓ Government/Regulatory Agencies:

- Do you need to deal with government agencies/ departments on a regular basis? What happens if your main contact is not available? Do you have an alternate contact?
- Is your business regulated? Does your company have compliance issues? If an emergency happens, who do you call? Make sure you have this information centrally located and easily recoverable.

Make sure when preparing your lists to Include: key contact name; work phone; cell phone; home phone; email; social media page/handle; alternate contact name; alternate contact phone; and alternate contact email.

TAKE ACTION NOW

4. Develop a **Key Vendors/Suppliers List**

Vendors/Suppliers:

- Which vendors/suppliers are important to your operations?
- Talk with your critical suppliers, discuss various risks to your supply chain and ask if they have any preparedness plans in place.
- What kind of planning has your landlord done in the event of an emergency? Do you have contact information for the landlord for an emergency at night or on a weekend? How about your lawyer and your insurance agent?
- Understand where you fit in the overall supply chain before the final product gets to the customer. Others may be relying on you to provide them with a product or service.
- Identify alternate supply chains for your critical goods and services. If you only have one supplier for a particular service, this could lead to a “single point of failure” if you are relying on them, and they become unavailable. It is important to build in redundancy in advance, so you will have options.
- Keep in mind that in an emergency situation changes may occur in how your suppliers might ship to you, credit might not be available and/or there might be a change in their handling of physical goods.
- Refer to the Key Vendors/Suppliers List template at the end of this section.

5. Develop a **Visitors List**

Visitors:

- While this group may not be critical to your business operations, it is important for you to know when they are physically on your business premises, as you may be liable for their safety. They may be family members of an employee, existing or potential customers, maintenance people, regulators or members of the public.
- Having a visitor sign-in policy to track arrivals and departures is one way to address this.

- Refer to the Visitors List template at the end of this section.

6. Develop a **Partners/Partnerships List**

Partners/ Partnerships:

- In this case, it does not refer to legal partners of the business. It refers to organizations like trade groups, like minded businesses, non-profits, community organizations, government, etc. who share your interest in serving the community. It is also those firms with whom you may be collaborating for marketing or joint purchasing.
- It may be an event or community group that you are associated with as a sponsor, supplier, or supporter.
- You may have resources (e.g. space, volunteers, equipment etc.) you can share with them during a time of disaster or vice versa.
- Refer to the Partners/Partnerships List template at the end of this section.

7. Develop a **Crisis Communications Plan**

Communication is always one of the biggest challenges in a crisis. Once you have your lists then having a strategy in advance to communicate with those on the lists will help you protect your assets. Elements of your strategy should include:

- Identifying a spokesperson (and alternate) who can comment on behalf of your business.
- Developing key messages to internal and external groups. This will tie into your Crisis Communications.

For example:

- Employees will want to know whether they will still have a job; when and where to report for work; if their jobs will change during the disaster; how to prepare to work in the new environment; response and recovery procedures; what to say to customers; and how and when they will be paid.
- Customers will need to know if your products/ services will still be available; opening hours; how can they contact you; delivery schedules etc.

TAKE ACTION NOW



- Create standard templates for press releases, news releases, employee updates, social media posts etc.
- Provide consistent, accurate, timely updates to your various internal and external groups.
- Monitor social media and websites for potential issues. Respond to rumours quickly.
- Refer to the Crisis Communications Plan template at the end of this section.

8. Provide an **Emergency Kit** for your People

People are the priority in an emergency. Be sure that you have on hand the items needed to shelter in place and/or escape a building.

- Refer to the Emergency Kit Checklist template at the end of this section.



Provide an Emergency Kit for your People



TEMPLATE

CRISIS COMMUNICATIONS PLAN

Purpose of the Plan:

To create guidelines for the business to communicate internally and externally in the event of a crisis, incident, or emergency to ensure that we are sharing timely and accurate information.

- **Identify Crisis Response Team Members.** Who will lead your efforts? What are the Team roles and responsibilities? Who will communicate with internal and external audiences including the media? Make sure you have backups identified, current work, home, and cell phone numbers, and email information.
- **List your Key Internal and External Audiences.** This can be pulled from the lists your developed in the Protect People section of this Business Emergency Continuity Plan. This should include: customers, survivors impacted by the incident and their families, employees and their families, news media, community—especially neighbors living near your facility, company management, directors and investors, government elected officials, regulators and other authorities, suppliers etc.. Include as much information for each contact as possible (e.g., organization name, contact name, business telephone number, cell number, fax number and email address).
- **Develop Key Messages based on your Hazard Risk Profile.** First determine what is happening, and why it is happening, as this will be important information to convey to your internal and external audiences. What do you want them to do about it? There are many different scenarios but your need to communicate will relate more to impacts or potential impacts of an incident on your business. For example:

 - Accidents that injure or kill employees or others;
 - Property damage to your facilities;
 - Production or service interruptions;
 - Chemical spills or releases with potential; environmental consequences; and,
 - Product quality issues.
- **List your Key Communications Channels** What are the key channels available to communicate your key messages? For example: email, phone texts, website, social media (Facebook, Twitter, LinkedIn, Instagram), local television, local newspaper, community Facebook pages, public notification systems etc.
- **Develop a List of Media Contacts.** List current contacts, including their organization, email, phone and Twitter handle.
- **Understand when to Activate.** If the incident is going to interfere with normal day to day operations, and presents a threat to your staff, property or brand reputation, you need to activate your plan. Who can activate your plan, and under what circumstances? Some basic principles to remember when you activate:

 - Communicate quickly;
 - Be timely and tell media/stakeholders when they can expect to hear from you next;
 - Communicate only about the crisis and your response to it;
 - Be consistent; and,
 - Get to the point quickly and focus only on relevant content.
- **Develop Templates in Advance.** This includes templates like media advisories or news releases. Develop them based on the types of scenarios most likely to occur, and think about how you will change your messages based on whether the impact to your business is low, medium or high. Also, have a holding statement ready to go. Something like “we have a crisis and we are working to get information together and will be sharing once we know more”.
- **Monitor the Crisis as it Unfolds.** Update your plan as required.

TEMPLATE

EMERGENCY KIT

- First Aid Kit
- Local Maps
- Battery-Powered or Hand Crank Radio
- Extra Batteries
- Wind-Up Flashlights
- Light Sticks
- Small Axe
- Hammer
- Hard Hat
- Whistle
- Non-Perishable Food
- Utensils
- Paper Supplies
- Manual Can Opener
- Plastic Bags
- Basic Tools (E.g., Screwdriver, Hammer, Etc.)
- Bottled Water In Non-Breakable Containers
- Dust Mask to Filter Contaminated Air
- Hand Sanitizer
- Rubber Gloves
- Blankets

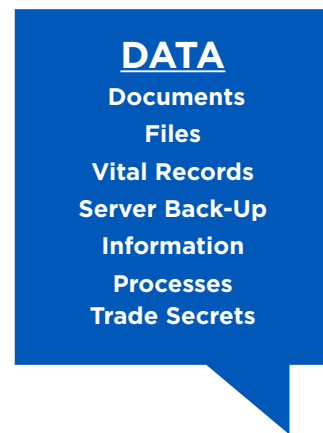
Other:



PROTECT DATA

No matter where your data is stored (in your head, in print, on servers, or in the cloud) you need to protect it. Data should be in an electronic format or printed as vital records. It can also be in the heads of your key people or in the very processes you use to run your business. It is important for a business to record and manage its data to maintain critical business functions during and after a disaster.

Note that just because you have a third-party vendor like Norton or Drop Box, does not mean you have adequate security measures in place to protect your data assets.



TAKE ACTION NOW

ACTION: Develop a Data Protection Plan

- Determine all the critical information about your business that is not currently written down - consider the knowledge that your key managers “just know” through their experience. Also consider key processes and trade secrets that are your competitive edge. Write it down.
- Identify your existing important documents and digitize them.
- Inventory your physical data assets and where they are located.
- Task someone to lead your data protection efforts.
- Back up your data.
- Secure your data.

ACTION: Assemble an Emergency Business Data Kit

Ideally, you should compile all your printed vital documents in a container that is waterproof and fire-proof. Refer to the Emergency Business Data Kit below for a list of supplies to include in your kit. You should also determine the following in advance:

- Who is responsible to assemble and maintain your emergency business data kit?
- Who is responsible to bring the emergency business data kit if you are evacuated?
- Refer to the Emergency Business Data Kit template at the end of this section.

It is important for a business to record and manage its data to maintain critical business functions during and after a disaster.



TEMPLATE

PROTECT DATA

Emergency Business Data Kit

- Emergency Action Plan, Business Continuity Plan
- Back up hard drives of digital information
- Emergency phone numbers, Employee Contact List
- Documents required to make decisions: legal documents (e.g. contracts, agreements), lease agreements, bank/financial account records, insurance policies
- Key(s), space plan and power requirements, locations of power/gas service
- Suppliers of critical equipment, equipment details (reorder and repair information)
- Priority inventory list including photos of your assets
- Cash and ATM/credit card(s)

TYPES OF CYBER ATTACKS

Here are some types of cyber attacks that every business needs to protect against and tips on how to do this.

Malware - Malicious code. Avoid clicking links or downloading attachments from unknown senders, have updated firewalls and computer operating systems.

Man-in-the-Middle (MITM) - A third party who gets between you on your mobile phone and a website you are visiting to get sensitive information. Avoid by using encrypted wireless access points that use WPA or greater, make sure sites use HTTPS connection.

Password Attacks - Third party trying to break into your systems by figuring out your password. Avoid by having strong passwords that you change regularly.

Denial of Service (DDoS) - Sends high volumes of traffic to a network to overload it and take it down. Avoid by staying current with software updates and monitoring flow of data to catch any spikes.

Phishing - Poses as a trusted third party to get your personal info via email. Avoid by verifying email requests over the phone, using a confirmed number you already have.

Malvertising - Malicious code that is downloaded when you click on ad. Avoid by not clicking on ads for free stuff and giveaways.

Rogue Software - Malware hidden as valid and necessary security software. Avoid with updated firewall, anti-virus or anti-spyware software programs.

PROTECT OPERATIONS

Operations are the core functions your business does daily.

OPERATIONS

Sales
Accounts Receivable
Accounts Payable
Computer Hardware/
Software
Medical Services
Mail Room
Manufacturing
Food Preparation
POS

TAKE ACTION NOW

ACTION: Develop your Hazard/Risk Profile

Every business is vulnerable to hazards and potential disasters. The most common are natural disasters and manmade disasters. It is important to list all hazards relevant to your business, regardless of whether it is a cause or effect of another hazard.

- Ask yourself these questions to determine the information you will need to restart after a disaster:
 - What pieces of your business need to be brought back as soon as possible after an interruption to remain open and reduce losses? For example: sales, accounts receivable and payable, computers, mail room, manufacturing, food preparation, sales, transportation of goods etc.
 - Which functions must be restored immediately, and which ones can be brought back later?
 - Are you able to assess impacts of specific hazards/risks that would most affect your critical business functions, and try to prepare for, and mitigate potential impacts in advance?
 - Is your business driven by demand from individual customers?
 - Do you have service-level contracts to maintain?
 - Do you have to adhere to regulations to operate your business?
 - Does your business depend on a specific power source (gas, electricity)?
 - Does your business depend on the specific skills of your employees?
 - Do you have an emergency cash reserve fund to purchase supplies, equipment or to relocate the business? How much cash would you require to survive a shutdown?
- Will you have access to a line of credit or credit card if you do not have enough emergency cash?
- Which financial obligations or expenses will need to be paid even if a disaster strikes?
- Will you be able to continue to accept payments from customers for accounts receivable?
- Do you have a payroll continuity plan in place for employees? Are your employees aware of payroll policies that will be in place during a disruption?
- Do you have adequate insurance in place (e.g. physical damage including inventory or buildings, business interruption or loss of income, data loss, liability claims etc.)? Do you understand your coverage, deductibles, limits, and how to file a claim?
- Will your employees be able to work remotely in case they are unable to work onsite for a short or longer period?

Typical actions taken to resume operations after a disruption:

- Implement Recovery Business Plan
 - Revision of Financial Plans
 - Adjust Marketing & Sales to New Conditions
 - Tailor Operations
 - Emphasize Customer Service via all means available
 - Adjust Staffing and Skill Sets
 - Review cash flow, inventories, employees, supply chain and insurance.
- Refer to the Hazard/Risk Profile template at the end of this section.



TEMPLATE

PROTECT OPERATIONS

Hazard/Risk Profile

- Identify types of risk specific to your business:
 - Natural disasters:** flood, lightning strike, hurricane, hail, tornado, earthquake, severe winter weather, wildfire, landslide.
 - Manmade:** data entry error, cyber attack, terrorism, vandalism/sabotage, theft/crime, security breach, epidemic, accident, civil disorder, hazardous material, active shooter/workplace violence, chemical spill, utility or

telecommunications disruption, loss of premises, fraud, software/hardware failure, labour unrest, loss/illness of staff, supply chain disruption, access to premises impeded by third party.

- Assess hazard/risk impact on your Critical Business Functions.
 - Highlight areas of greatest risk
 - Rate potential hazards and risk in each area:
- Negligible = 1, Marginal = 2, Critical = 3, Catastrophic = 4

IMPACT TO CRITICAL BUSINESS FUNCTIONS							
	People	Data	Building	Inventory	Equipment	Operations	Score
Accident							
Computer Virus							
Cyber Threat							
Earthquake							
Fire							
Flood							
Hurricane/Typhoon							
Plane Crash							
Power Outage							
Storms							
Terrorism							
Theft/Security							
Thunderstorm/Lightening							
Tornado							
Tsunami							
Volcanic Eruptions							
Critical Family Incident/loss							
Personal Illness/Injury							
Supplier Bankruptcy							
Pandemic							
Totals							
	Priority	Priority	Priority	Priority	Priority	Priority	

- Prioritize Critical Operations & Processes

PROTECT EQUIPMENT

Your equipment refers to physical items required for your business to provide its products and services. This includes things like servers, manufacturing and specialty equipment, furniture, copiers, office supplies etc. It may overlap with your Inventory Items.

EQUIPMENT

Servers
Network
Manufacturing
Equipment
Specialty Equipment
Furniture
Copiers

TAKE ACTION NOW ▶▶▶▶▶▶▶▶▶▶

ACTION: Prepare an **Equipment List**

- Prioritize your most important equipment.
- What is critical for your operations to continue? How will you protect the equipment?
- Continually update equipment inventory.
- Refer to the Equipment List template at the end of this section.



Prioritize your most important equipment.



TEMPLATE

PROTECT BUILDINGS

BUILDINGS	
Building Information	
Type of physical structure (warehouse, main office, store front, lease space, storage unit, loading dock, home, high rise, low rise, converted house etc.).	
Year it was built. Is it in good condition or does it need repair.	
Type of construction (e.g. wood, brick, steel).	
Property/building documents available (e.g. blueprints, structural engineer's report, geotechnical soil report, site disaster history).	
Access points for essential services (water, electrical, gas).	
Process to shut off the essential services.	
Do you lease or own the building? What happens in the case of a disaster, who is responsible for what.	
Type of property insurance in place.	

TEMPLATE

PROTECT BUILDINGS

Emergency Action Plan

EMERGENCY ACTION PLAN			
	NAME/S	Work and Cell Phone Numbers	Work and Home Email Addresses
Who is on your emergency planning team? List them all.			
Add the people from neighboring businesses and the building management who will participate in your emergency planning team. List them all.			
Who is your primary crisis manager?			
Who is your alternate crisis manager?			
Who calls first responders (e.g. fire, paramedics, police etc.)?			
What is your process for reporting emergencies/ fires?			
Will anyone onsite be able to perform rescue or medical duties? If so who? Who is their backup?			

CORPORATE POLICIES, DOCUMENTS AND INFORMATION	
What is your evacuation policy and procedure? Who goes out which door? Do you have floor plans or maps that can help people understand where to go?	
For employees that need to continue or shut down critical operations, do they know how to operate fire extinguishers, or perform essential services that cannot be shut down during an emergency?	
How will you notify employees that they need to evacuate or take other action? Do you have an intercom system?	

TEMPLATE

PROTECT BUILDINGS

Emergency Action Plan



CORPORATE POLICIES, DOCUMENTS AND INFORMATION

Where is your muster point outdoors? How do you account for employees once evacuated?	
How will you handle those with physical handicaps?	
If your location is not accessible, where will you operate from? Who is responsible for issuing the 'all clear'?	
Do you have alarms on site? Are they working? Can everyone hear them?	
How many times will you practice evacuation procedures each year?	
How is this knowledge transferred to new employees?	

OTHER ENCLOSURES/ATTACHMENTS

Emergency Contacts List	
Facility maps, including exits and muster points	

GENERAL INFORMATION

BUSINESS INFORMATION

To be made accessible to employees and first responders.

Company Legal Name:

Company Operating as:

Owner:

Business Address:

City: Province: Postal Code:

Business Phone Number:

Emergency Phone Number 1: Name:

Emergency Phone Number 2: Name:





List of revisions:

It is important to update your Business Emergency Continuity Plan on a regular basis. By tracking revisions and dates it is easier to keep track of the most current version. Be sure to include the revised copy in your Business Emergency Data Kit.

Consider the following questions, as part of that review process:

- Is all the contact information up to date?
- Have any procedures or priorities changed?
- Have any roles or responsibilities changed?
- When will the next update of the plan take place?

Revision Number	Details	Revised by	Revision Date

The following individuals have received copies of the most current Business Emergency Continuity Plan:

Name	Details	Date



BUSINESSLINK



This document is based on the intellectual property of
Leann Hackman-Carty, MYD Global
enhanced by **Natalie Gibson, InnoVisions & Associates**
for use by **Business Link**.