

Plan to Stay in Business



An Emergency Planning Guide

Why this plan is Important for Your Business

Every year emergencies and other disasters take a heavy toll on business and industry – in lost sales, wages, and infrastructure, not to mention lives. When that happens, business managers and owners often realize a profound sense of powerlessness. There is nothing worse than knowing that years of hard work can be reduced to rubble in a matter of seconds.

There are many things business owners can do to avoid feeling powerless and at the mercy of chaotic and uncontrollable events swirling around them. You can start to inoculate yourself and your business from disaster by taking charge and beginning your planning and preparations for the worst. This booklet will help you do precisely that.

This workbook, also known as a Business Continuity Plan (BCP), when applied to your organization will ensure you are uniquely positioned to limit damages, reduce potential injuries, prevent deaths among your workers, preserve sales with your customers and return to normal operations more quickly.

America’s businesses form the backbone of our nation’s economy. A commitment by the “whole community” to planning today will help support employees, customers, the community, and the economy throughout the state, our nation and even globally.

How quickly an individual business can get back to normal operations after an incident is directly related to the amount of emergency planning done before the event. Though each situation is unique, any organization can be better prepared if they plan carefully, put emergency procedures in place, work with their emergency management partners, and develop plans for a wide variety of potential emergencies.

The ***Plan to Stay in Business: A Guide to Developing Your Own Business Continuity Plan***, is a simple 5 step program with supporting checklists that you can use to ramp up your own disaster planning and tailor a program that fits your operational and emergency planning needs. While there is no guarantee that using this booklet will save your business from any calamity, its use does stack the odds more in your favor than they would be otherwise. No matter if your business is a small “Mom and Pop” shop or a large corporation with thousands of employees and multiple locations, this guide is intended to get you started on your own path away from that of a hapless victim, to an active participant in your businesses long term success.

Public Private Partnerships
Idaho Office of Emergency Management
4040 Guard St., Bldg. 600
Boise, ID 83705

Plan to Stay In Business

YOUR BUSINESS CONTINUITY PLAN

| | | | |
|---------------|--|--------------|-------------------|
| STEP 1 | Assess Hazards That Could Affect Your Business Identify the hazards that are most likely to affect your business and plan for those first. | 2-4 | STEP 1 |
| STEP 2 | Have a Plan How quickly your company can return to business after an event can depend on emergency planning done today. | 5-7 | STEP 2 |
| STEP 3 | Protect Your Investment It is important to safeguard your company’s physical assets. | 8-9 | STEP 3 |
| STEP 4 | Know How to Respond Determine how your business will respond to emergencies. | 10-11 | STEP 4 |
| STEP 5 | Talk to Each Other One of the best ways to ensure the recovery of your company is to provide for the well-being of your Co-workers. | 11-12 | STEP 5 |
| | How You Can Help in Your Community | 12 | HELPING |
| | Checklists | | CHECKLIST |
| | Recovery Overview | 13-16 | |
| | What to take when you evacuate | 17-18 | |
| | Specific threat checklists | 19-34 | |
| | Vendor Vulnerability Assessment | 35-37 | ASSESSMENT |
| | Additional information | 39 | ADDITIONAL |

STEP 1. ASSESS HAZARDS THAT COULD AFFECT YOUR BUSINESS

STEP 1

Consider the potential impacts of hazards when developing your emergency plan. You can use the Vulnerability Analysis Chart as a tool to guide the process, which entails assigning probabilities, estimating impact and assessing resources, using a numerical system.

Vulnerability Analysis Chart

Rate each criterion on a scale of 1 to 5 with 1 being low and 5 being high.

| Type of Emergency | Probability | Human Impact | Property Impact | Business Impact | Total |
|-------------------|-------------|--------------|-----------------|-----------------|-------|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

A. List Types of Emergencies

In the first column of the chart, list all emergencies that could affect your facility, including those identified by your local emergency management office. Consider both:

- Emergencies that could occur within your facility
- Emergencies that could occur in your community

Below are some examples of emergencies or events to consider:

- Fires
- Power/Utility Outages
- Severe weather
- Cyber Attacks/Malware/Ransomware

- Hazardous material spills
- Transportation accidents
- Earthquakes
- Infectious Disease Outbreaks
- Loss of key staff

Consider what could happen as a result of:

- Prohibited access to the facility
- Loss of electric power
- Loss of Communications
- Loss of Critical Computer Systems/Critical Data
- Ruptured gas mains
- Water damage
- Smoke damage
- Structural damage
- Air or water contamination
- Explosion
- Building collapse
- Trapped persons
- Chemical release

B. Estimate Probability

In the Probability column, rate the likelihood of each emergency's occurrence. Use a simple scale of 1 to 5 with 1 as the lowest probability and 5 as the highest.

C. Assess the Potential Human Impact

Analyze the potential human impact of each emergency -- the possibility of death or injury. Use a 1 to 5 scale with 1 as the lowest impact and 5 as the highest.

D. Assess the Potential Property Impact

Consider the potential for losses and damages. Again, assign a rating in the Property Impact column, 1 being the lowest impact and 5 being the highest.

Consider:

- Cost to replace
- Cost to set up temporary replacement
- Cost to repair

Example: A bank's vulnerability analysis concluded that even a "small" fire could be catastrophic to the business due to a computer system failure. The planning group discovered that bank employees did not know how to use fire extinguishers, and that the bank lacked any kind of evacuation or emergency response system.

E. Assess the Potential Business Impact

Consider the potential loss. Assign a rating in the Business Impact column. Again, 1 is the lowest impact and 5 is the highest.

Assess the impact of:

- Business interruption/loss of critical business functions
- Employees unable to report to work
- Customers unable to reach facility
- Company in violation of contractual agreements
- Interruption of critical supplies
- Interruption of product distribution

Add the Columns

Total the scores for each emergency. The lower the score, the better. While this is a subjective rating, the comparisons will help determine planning and resource priorities.

When assessing resources, remember that community emergency workers -- police, paramedics, firefighters -- will focus their response where the need is greatest, or they may be victims themselves and be unable to respond immediately. That means response to your facility may be delayed.

STEP 2. HAVE A PLAN

Decide who should participate in developing your emergency plan and assign a team leader.

- (Name/Title/Department)
- (Name/Title/Department)
- (Name/Title/Department)
- (Name/Title/Department)

Continuity of Authority. List the Primary Contact as well as alternates.

Primary Contact

Name: _____

Phone Number: _____

E-Mail: _____

If the Primary Contact Person is unable to manage the event, the person below will succeed in management:

Alternate Contact (2)

Name: _____

Phone Number: _____

E-Mail: _____

- Assumes Command
- Assesses the situation
- Activates emergency procedures
- Coordinates employee communications
- Other/Describe: _____

If the Alternate Contact Person is unable to manage the event, the person below will succeed in management:

Alternate Contact (3)

Name: _____

Phone Number: _____

E-Mail: _____

- Assumes Command
- Assesses the situation
- Activates emergency procedures
- Coordinates employee communications
- Other/Describe: _____

Local Emergency Contact Information:

(Dial 9-1-1- in an emergency for local or isolated emergencies)

Building/Property Manager: _____

Building Security: _____

Telephone Company: _____

Gas/Heat Company: _____

Electric Company: _____

Information Technology (I.T.) Contact: _____

Insurance Company: _____

County Emergency Management: _____

STEP 2

Identify necessary resources to keep your business operating such as:
Staff, materials, procedures, contacts, equipment (additional pages may be needed):

| Resource/Function | Contact Information | Alternate |
|-------------------|---------------------|-----------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

STEP 3. PROTECT YOUR INVESTMENT

Identify Critical Business Functions

- Identify alternates to perform critical functions
- Provide training and equipment to ensure the alternates can perform the functions
- Consider developing job aids such as checklists to assist alternates in performing those duties.

Keep copies of important records off-site such as:

- Building plans
- Pictures of the facility-inside and out
- Insurance policies
- Employee contact and identification information
- Bank account records
- Tax records
- Supplier and shipping contact lists
- Off-site back ups of computer data

Alerts and Warnings

- Monitor the media in the area
- Enroll in the Idaho State Alert and Warning System (ISAWS)
www.ioem.idaho.gov

Insurance

- Review and understand what your policy covers
- Keep in mind the cost of rental equipment, temporary workers, data recovery etc.
- Find out what records your insurance provider will want to see and store them off-site with your important documents

Utilities

Plan for disruptions of utilities such as:

- Electricity
- Gas
- Telecommunications
- Water
- Sewer

Fire Safety

Fire is the most common of all business disasters.

- Install smoke alarms, smoke detectors, and fire extinguishers
- Discuss who will alert the fire department and how they will do it
- Plan and discuss how to evacuate in the event of a fire. Consider:
 - Fire exits
 - A safe place for all to meet for accountability

Improve Cyber Security

Protecting your data and information technology system may not require experts. Some things you can do:

- Use anti-virus software and keep it up to date
- Do not open e-mail from unknown sources
- Back up your data and store it off-site on easily transportable devices such as external hard drives.
- Subscribe to the Department of Homeland Security National Cyber Alert System to receive free timely alerts on new threats and learn how to protect yourself in cyberspace <http://www.us-cert.gov/>

STEP 4. KNOW HOW TO RESPOND

Evacuation – If local authorities tell you to evacuate, do so immediately.
(SEE PAGE 17)

Identify who internally will:

- Order an evacuation of your business
- Shut down critical operations
- Lock doors
- Designate assembly sites for all workers, visitors, and customers
- Develop a system to account for everyone on your site
- Provide an "all clear" or "return to work" notification

Shelter In Place – In some emergencies, you may be asked to shelter in place. Act quickly and follow instructions.

Identify who internally will:

- Order all to shelter in place
- Close all doors and windows
- Turn off ventilation systems
- Seal doors and windows

There are some steps you can take to help protect your assets every day.

Secure Facilities and Buildings

- Secure entrances and exits
- Plan for mail safety
- Identify which equipment is necessary to keep your business running such as:
 - Machinery
 - Computers
 - Custom parts
- Plan how to transport, replace or repair vital equipment if it is damaged or destroyed
- Store extra supplies, materials, etc.

Secure your Equipment

The force of disasters like fires, floods and earthquakes can damage or destroy important equipment

- Conduct a room-by-room walk through to determine what needs to be secured
- Attach equipment and cabinets to walls or other stable locations
- Elevate equipment off the floor to avoid electrical hazards and damage in the event of flooding

STEP 5. TALK TO EACH OTHER

One of the best ways to ensure your company's recovery is to provide for the well-being of your co-workers

- Talk with staff frequently and practice what you intend to do during and after an emergency
- Set up a telephone tree, e-mail alert, text messaging, or call in alert to leave an "I'm okay" message (Text messaging has proven to be the most successful)
- Cross train if possible. Identify alternates to perform critical functions.
- Include emergency preparedness information available at www.ioem.idaho.gov in staff meetings or new employee orientations
- Encourage your employees to develop a plan for emergencies at home

Prepare for Medical Complications

- Keep first-aid supplies in stock and easily accessible
- Encourage employees to take basic first-aid and CPR training
- Be sure to include people with disabilities in emergency planning

Support Employees after an Event

Getting back to work is important to personal recovery. Some things you can do:

- Reestablish routines as soon as possible
- Create opportunities where co-workers can talk openly about their experiences, fears and anxieties
- Allow employees time at home to care for their families

HOW YOU CAN HELP IN YOUR COMMUNITY




We will be able to enhance our service to our neighbors, citizens, first responders and those affected by disasters when public and private sector representatives work together on the same team.

- Get involved with your local, tribal and state Emergency Management Organizations. Emergency Management telephone numbers can be found at:
 - State Emergency Management
<https://ioem.idaho.gov/about/contact/agency-contacts/>
 - County and Tribal Emergency Managers
<https://ioem.idaho.gov/about/contact/county-tribal-emergency-managers-contacts/>
- Attend Local Emergency Planning Committee (LEPC) meetings
- Participate in training and exercises provided at no cost by your jurisdiction and the state.
- Assist in the development of protocols to integrate businesses into emergency management.
- Share resources during an incident or a disaster
- Be prepared and be involved

RECOVERY OVERVIEW

Disaster planning is vital to a successful recovery. The following checklist is a comprehensive outline of the disaster recovery process. Before you begin, it is prudent to outline a schedule and budget.

| | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | Recovery Team |
| | Determine a primary and back up Crisis Manager |
| | Determine a primary and back up Recovery Management Team |
| | Establish and notify employees involved in recovery and clarify roles. |
| | Communicate recovery action steps to all employees. |
| <input checked="" type="checkbox"/> | Risks and Hazards |
| | List natural and man-made events that may impact your business. |
| | Rate the likelihood of occurrence for each event |
| <input checked="" type="checkbox"/> | Alternate Location |
| | Locate and confirm an alternate recovery location and back up location. |
| | Develop relationships with recovery vendors and/or neighboring businesses. |
| | Assess suitability of other branches or locations for recovery. |

| | |
|---|--|
| | Set aside space for an emergency command center |
|  | Communications |
| | Develop a plan to communicate both internally and externally (including the media) |
| | Create an employee phone tree and store copy(s) off-site. |
| | Record and store external emergency contact information (electric, plumber, insurance, etc.) |
| | Determine plan for re-routing critical existing phone lines and numbers. |
| | Ensure plan includes multiple methods of communication (text, email, cell phone, social media, etc.) |
|  | Employees |
| | Establish a plan for emergency payroll |
| | Develop a password-protected page, email or a voice recorded emergency communication system. |
| | Engage people with disabilities in your emergency planning. |
|  | Technology and Data |
| | Document technology hardware, software and licensing information. |
| | Develop technical recovery procedures to be followed in the event of an interruption. |

| | |
|-------------------------------------|--|
| | Determine and list individuals/vendors to manage technical recovery. |
| | Determine source for back up technical resources (PCs, servers, printers, phone systems, etc.) |
| | Document critical data to be restored and back up all data at off-site location |
| <input checked="" type="checkbox"/> | Operations |
| | Document critical business functions |
| | Develop a plan to restore critical business functions. |
| | Determine employees responsible for restoring each critical business function. |
| | Create a crisis management plan. |
| | Develop a plan for expedited financial decision-making and disaster cost tracking |
| | Review insurance coverage and assure it is adequate for all possible disasters. (Take into consideration property value appreciation and construction materials inflation since your last review.) |
| <input checked="" type="checkbox"/> | Supply Chain |
| | Develop plan to communicate with vendors and suppliers |
| | List key clients, suppliers, and critical recovery contacts and store copy(s) off-site. |
| | Assure key vendors and suppliers have actionable recovery plans. |

| | |
|-------------------------------------|---|
| | Develop relationships with alternate suppliers in case primary vendors are unavailable. |
| <input checked="" type="checkbox"/> | Safety |
| | Assemble a disaster recovery kit. |
| | Create an evacuation plan (See page 17 in this document). |
| | Create an emergency shelter plan. |
| <input checked="" type="checkbox"/> | Testing and Maintenance |
| | Test the disaster recovery and business continuity plan. |
| | Conduct a post-test review and report results. |
| | Refine, tweak and adjust plan as needed. |
| | Make sure as new employees are brought into your business they are trained/ briefed on these plans. |
| | Communicate changes to the plan to all employees as warranted. |


WHAT TO TAKE WHEN YOU EVACUATE

When an evacuation takes place at work, employees often don't know what to take with them and what to leave behind. You've heard the terms before: "Bug Out", "Go Bag", "Grab Bag" and more. These are all terms to describe quick access emergency kits that hold all your important tools and possessions in a single, easy to reach location.

In order to make your recovery as smooth as possible, we encourage you to educate your employees on the items they may want to bring with them in the event of an evacuation. To help you with this process, we have created the following checklist of suggested items. Keep in mind, these are just suggestions. This is not a complete list, nor are we suggesting that you plan to carry all these items. Some may be unnecessary or not applicable in your personal situation. Remember, above all, your own safety and the safety of others should be your primary goal.

Here are a few tips to keep in mind when planning for an evacuation.

- The items you would like to include in your "go bag" should be close by, always. Time wasted collecting items before evacuating could be a serious, even deadly mistake.
- The items you plan to take with you should be easily accessible and easy to carry – hence the suggested use of a bag to contain them all in one place.
- This collection of tools and possessions should be the bare minimum you would need in the event of a crisis taking place in your office or business.


| | |
|--|---|
|  | Suggested Items to include in an Business/Office Evacuation "Go Bag" |
| | Cellphone or PDA, containing key emergency contacts, passwords, etc., and charger |
| | Identification and wallet/cash/credit cards |
| | Car/House keys and office keys or pass card |
| | Laptop & Charger |
| | Office Phone Roster (including personnel emergency contacts' information) |
| | Office Floor Plans (to aid in possible search/rescue efforts) |

| | |
|--|---|
| | Calendar/Day Planner |
| | Server Back up Tapes or Drives |
| | Disaster Plan or Emergency Procedure Manual |
| | Emergency plans/procedures, asset inventors, insurance information/policies |
| | Flash Drive with critical documents, employee information |
| | First-aid Supplies |
| | Any Personal Medications |
| | Password Book/Document |
| | Basic Office Supplies (pen & paper) |
| | Network Cables (Ethernet) |

Above all, any evacuation plan, emergency procedure, or disaster plan should protect the safety and well-being of all employees and guests in your office. However, those who take the extra time to keep important belongings and tools close at hand in the event of an emergency may recover from a disaster more quickly and easily with these items in their possession.

WINTER WEATHER PREPAREDNESS CHECKLIST

Winter weather brings concerns about heat and maximizing its retention, frozen pipes, and access to your place of business. The following checklist will help you identify the areas of your business that are most susceptible to winter hazards and to suggest ways to minimize damage. It is a good idea to develop a plan of action for your business and your staff to be ready for this type of interruption. Below you will find critical information and preparedness tools to assist in protecting your business and the most critical element of your business – your employees.

| | |
|---|--|
|  | Before the Storm |
| | Check your insurance coverage for protection against winter hazards. Also consider asking your agent about an "All Hazards or "All Risk" policy and make sure you understands what "exclusions" may apply. |
| | Develop a procedure for restoring electrical services on an item-by-item basis. |
| | Develop a procedure for relocating salvageable and undamaged stock and supplies. |
| | Add the following supplies to your disaster supplies kit: rock salt (to melt ice on driveways), sand (to improve traction), and snow shovels (or other snow removal equipment). |
| | Determine your greatest risk potential: loss of heat, frozen pipes, and/or loss of access due to snow/ice. |
| | Identify who is responsible for keeping heating equipment in good working order: business owner or landlord. |
| | Identify who is responsible for snow/ice removal: business owner or landlord. |
| | Determine what equipment needs to be protected from freeze-up, i.e. computers, telecommunications, manufacturing equipment, etc. |
| | Are portable heaters or other emergency equipment needed? |
| | If snow and/or ice prohibit access to your business, are there alternative ways to enter your premises? |


| | |
|--|--|
| | Seal all openings with caulking and insulation where cold air can enter. |
| | Repair walls and roofs to prevent drafts; inspect roof drains for debris. |
| | Make sure storm windows are effective, if appropriate. |
| | Make sure heating equipment is in good condition and operating efficiently. Consider having it serviced by a licensed and qualified HVAC technician and company. |
| | Arrange for snow removal from driveways, doorways, and roofs. |
| | Drain all idle pumps and compressors, making sure jackets are vented. |
| | Provide proper lubrication on equipment for cold weather operation (i.e., emergency generators, snow blowers). |
| | Test cold weather equipment. |
| | Clean and inspect boilers and firing mechanism/controls. |
| | Maintain automatic sprinkler protection in idle buildings; promptly handle sprinkler system impairments; notify local fire department. |
| | Monitor building temperature especially in hard-to-heat areas containing vulnerable equipment. |
| | Keep temperatures above 40°F. |
| | Mark hydrants near your business for ease in locating and clearing after a heavy storm. |



During the Storm

Heaters, snow blowers, generators, and cold-weather equipment should be located where it is most likely to be used.

| | |
|--|---|
| | Keep driveways, walkways, and doorways clear of snow and ice. |
| | Open water faucets slightly to let them drip in order to keep water flowing through the pipes that are vulnerable to freezing. Ice may still form, but the open faucet helps prevent the pipe from bursting by allowing relief for any built up pressure. |
| | Names and phone numbers of your heating contractor, plumber, fire department, insurance agent, and building owner should be easily accessible. Have someone assigned to check indoor temperatures should your place of business be vacant for long periods of time. |

| | |
|---|--|
|  | Your Employees |
| | Ensure you have an emergency communication plan in place prior to the storm, evacuation, or threat. |
| | Have all employees, vendors, and client contact information on hand. |
| | During evacuation, consider your phones lines - redirection to cell phones, answering service, or Google Voice could be critical. |
| | Following the storm, notify all critical people of the next steps that will be taken, based on damage. |
| | Winter storms may range from a moderate snow in a short amount of time to a blizzard lasting for days. Some storms are regional and may affect several states, while others are more localized, depending upon geography and terrain. Common characteristics of winter storms are dangerously low temperatures, strong winds, ice, sleet, and freezing rain. |
| | Make sure your employees have implemented plans to keep their families safe and supplied |


Know the Terms:

- **Winter storm watch:** be alert, a storm is likely.
- **Winter storm warning:** take action, the storm is in or entering the area
- **Blizzard warning:** snow and strong winds combined will produce blinding snow, near zero visibility, deep drifts, and life-threatening wind chill--seek refuge immediately!
- **Winter weather advisory:** winter weather conditions are expected to cause significant inconveniences and may be hazardous, especially to motorists
- **Frost/freeze warning:** below freezing temperatures are expected and may cause damage to plants, crops, or fruit trees


EARTHQUAKE PREPAREDNESS


Idaho is a seismically active state. As such, earthquakes will continue to happen here and their impacts widely felt.

The following checklist covers some basic points to consider in preparing for an earthquake which will help you recover more effectively. In the aftermath of an earthquake, these contingencies will prove vital activities ensuring that any damage to your business and resources are minimized.


| | |
|---|--|
|  | <h2>Before the Earthquake</h2> |
| | <p>Be aware of your risk level. Add a map to your disaster plan and make sure everyone is aware of the earthquake risk level in your specified region.</p> |
| | <p>Think about communications. Chances are the phone company and possibly cell towers will be affected. Your disaster recovery/response team will need to be in immediate contact with one another to ensure that your plan is activated and moving forward as quickly as possible. Think about two-way radios or text messages as an alternative.</p> |
| | <p>Develop a plan around communication, and deliver this to your team. Be sure to clearly identify each individual's roles and responsibility prior to the earthquake.</p> |
| | <p>Implement structural and non-structural hazard mitigation actions: bolting furniture to walls, ensure hardware and technology are secure, safety latches for cabinet doors, install fire sprinklers, use hook and loop fasteners to keep computers and other equipment from falling.</p> |
| | <p>Discuss coverage with your insurance provider. Understand your extra expense, and business interruption policies, before the interruption occurs.</p> |
| | <p>Contact your property owner or facilities manager and ask about having a laminate or plastic film placed on the inside of the windows to prevent glass shattering and endangering employees.</p> |
| | <p>Assemble and store an emergency supply kit for 3 days minimum</p> |
| | <p>Assemble building site maps and floor plans identifying exits, fire escapes, stairways, utility valves and shut-offs, fire extinguishers, hydrants, standpipes, hazardous materials, and locked or restricted areas. Include these in your DR plan.</p> |
| | <p>Prepare your building for an extensive power outage and look at power options, particularly generator requirements. You may want to contact a local electrician for assistance with this.</p> |

| | |
|--|--|
| | Review your current data back up procedures and consider contracting with a datacenter or colocation facility that is in a different part of the country (one not prone to earthquakes, hurricanes or any other kind of aggressive natural events). Back up all your data to them on a daily (or at least every other day) basis, so that in the event you lose your networks and servers you can be back up and running and restoring your saved data to replacement equipment. |
|--|--|

| | |
|---|---|
|  | During the Earthquake |
| | If you are indoors , Drop, Cover and Hold. Drop down to the floor. Take cover under a sturdy desk, table or other furniture. Hold on to it and be prepared to move with it. Hold the position until the ground stops shaking and it is safe to move. Stay clear of windows, fireplaces, wood stoves, and heavy furniture or appliances that may fall over. Stay inside to avoid being injured by falling glass or building parts. If you are in a crowded area, take cover where you are. Stay calm and encourage others to do likewise. |
| | If you are outside , get into the open, away from buildings and power lines. |
| | If you are driving , stop if it is safe, but stay inside your car. Stay away from bridges, overpasses and tunnels. Move your car as far out of the normal traffic pattern as possible. If possible, avoid stopping under trees, light posts, power lines, or signs. |
| | If you are in a mountainous area , or near unstable slopes or cliffs, be alert for falling rock and other debris that could be loosened by the earthquake. |

| | |
|---|---|
|  | After the Earthquake |
| | Employees should immediately check for injuries among fellow workers and render first-aid. Seriously injured persons should not be moved unless they are in danger of further injury. |
| | Check for fire hazards, gas leaks, or damaged electrical wiring. Make sure main valves are turned off. |
| | Use flashlights (in emergency supply kit) vs. matches/lighters, due to potential gas leaks. |
| | Be prepared for aftershocks – these can come for several days after the main quake and can frequently topple already weakened structures. |
| | Consider relocation during recovery, depending upon damage to your structure. |


| | |
|--|--|
| | Bring all vital records with you to your recovery site: data, employee lists, vendor lists, etc. |
| | Following the earthquake, notify all critical people of the next steps, based on damage. |

| | |
|---|--|
|  | Your People |
| | Ensure you have an emergency communication plan in place prior to the event, evacuation, or threat. |
| | Determine who is certified in CERT, CPR, etc. and what their responsibilities will be in the event of an earthquake. |
| | Keep all employees posted on status and the next steps. |
| | During evacuation, have a central point of contact for all employees, and ensure you know where people are located. |
| | During evacuation, consider your phones lines - redirection to cell phones, answering service, or Google Voice, could be critical. |
| | Make sure they have implemented plans to keep their families safe and supplied |

FLOOD PREPAREDNESS

Floods are one of the most common and widespread of all disasters, and continue to grow in frequency and severity. In Idaho, floods are typically associated with the spring runoff, however they can strike at any time. Businesses are more likely to flood than burn down, so it is vital to prepare now.

The following checklist will help keep your business afloat even if the worst happens. Most businesses can save between 20% and 90% on the cost of stock and movable equipment by taking action to prepare in advance of flooding. The following resources and tools will help mitigate your risk and protect not only your business, but also the most critical element of your business – your people.

| | |
|---|--|
|  | Before the Flood |
| | Review the Emergency Plan with your team and key employees |
| | Take all necessary steps to prevent the release of dangerous chemicals that might be stored on your property. Locate the main gas and electrical shut-offs and anchor all fuel tanks. |
| | Postpone any receipt of goods - deliveries, couriers, etc. |
| | Contact insurance agent, discuss policy, etc. If you don't already have it, consider National Flood Insurance. Factor in the 30 day waiting period. Get more information at http://www.floodsmart.gov or by calling 1-800-427-4661 |
| | Establish emergency communication method (Alert Notification System, phone tree, etc.), identify meeting place and time for all key employees in Crisis Management Team, and create a voice mail for when evacuated, or out of office, etc. |
| | Update disaster recovery kits and begin crisis back up procedures |
| | Maintain accurate inventory of product on site |
| | Use plugs to prevent floodwater from backing up into sewer drains, or install flood vents/or flood proof barriers |
| | Stay tuned to local media & community messaging |

CHECKLIST




During the Flood

| | |
|--|--|
| | Life safety is paramount |
| | Begin the next phase of your business continuity plan |
| | Send non-critical staff home |
| | Raise elevators to the 2nd floor and turn them off. |
| | Stay tuned to local media - evacuate when required |
| | Take cell phones, charger, critical hardware, and emergency kits with you. Unplug electrical items before leaving. |
| | Consider your business phones and redirection to cell phones, an answering service, or Google Voice |



After the Flood

| | |
|--|---|
| | Listen for news reports to determine whether the community's water supply is safe to drink. |
| | Avoid floodwaters; water may be contaminated by oil, gasoline, or raw sewage. Water may also be electrically charged from underground or downed power lines. |
| | Be aware of areas where floodwaters have receded as roads may have weakened and could collapse under the weight of a car. |
| | Clean and disinfect everything that got wet. Mud left from floodwater can contain sewage and chemicals. Implement DR plan, and monitor local authorities' communication |
| | Contact employees via determined method of communication and discuss the next steps. |
| | Contact your insurance agent. |

| | |
|---|--|
|  | <h2>Your People</h2> |
| | <p>Ensure you have an emergency communication plan in place prior to the storm, evacuation, or threat.</p> |
| | <p>Have all employees, vendors, and client contact information on hand.</p> |
| | <p>During evacuation, have a central point of contact for all employees, and ensure you know where your employees are located.</p> |
| | <p>Following the flood, notify all critical people of the next steps, based on damage.</p> |
| | <p>Make sure they have implemented plans to keep their families safe and supplied</p> |

Helping to Mitigate your Risk for Flood Interruption:


Do You Know the Terms?


- **Flood Watch:** Flooding is possible. Tune in to NOAA Weather Radio, commercial radio, or television for information.
- **Flash Flood Watch:** Flash flooding is possible. Be prepared to move to higher ground. Listen to NOAA Weather Radio, commercial radio, or television for information.
- **Flood Warning:** Flooding is occurring or will occur soon. If advised to evacuate, do so immediately.
- **Flash Flood Warning:** A flash flood is occurring. Seek higher ground on foot immediately.


WILDFIRE PREPAREDNESS

Wildfire in Idaho is a common occurrence that results in untold millions of dollars in losses to business and the state economy. Impacts of a wildfire include direct property damage, cost of suppression and damage to personal property and natural resources. The severity of effects is directly related to the intensity and extent of the wildfire.

Below is a checklist of just some of the things to consider to prepare your business for such an event as well as to ensure the safety of the people within your organization.

| | |
|---|--|
|  | Before the Onset of a Wildfire |
| | Keep an adequate number of appropriate fire extinguishers in strategic locations (such as near loading docks and waste collection areas) and maintain them properly. |
| | Train employees on how to use extinguishers correctly. |
| | Ensure that your building has followed the “Firewise” protocols. This includes taking the time to remove unnecessary vegetation and “ladder fuels” that could make your facility more prone to catching fire. Wherever possible use non-combustible or fire-resistant building materials. |
| | Consider maintaining a water supply at your facility to control small fires until emergency personnel can arrive. You might install a water tank or install hoses and pumps to an existing pond, river or lake. Be sure the hoses are long enough to reach your building and inspect them regularly. |
| | If your business is located in an area subject to freezing temperatures, be sure that water outlets and pumps are protected. |
| | Evaluate water levels in extreme hot and cold weather conditions. |
| | If your water pump uses electrical power, consider obtaining a gasoline or diesel powered pump or generator in case the electricity is cut off during a fire. However, be aware of the risk of storing a large quantity of fuel. Use an appropriate storage facility that is protected against vehicle impacts and fire. |
| | Have appropriate tools, such as rakes, axes, saws, buckets and shovels, available to help control small fires while waiting for emergency personnel to arrive. |

| | |
|---|--|
|  | During a Wildfire |
| | Go to a pre-designated shelter area such as a safe room, basement, storm cellar, or the lowest building level. If there is no basement, go to the center of an interior room on the lowest level (closet, interior hallway) away from corners, windows, doors, and outside walls. Put as many walls as possible between you and the outside. Get under a sturdy table and use your arms to protect your head and neck. Do not open windows. Evacuation orders will often be swift and accurate for affected areas. However, if unable to evacuate, stay inside and away from outside walls. Close doors, but leave them unlocked in case firefighters require quick access into your area. |
| | Turn on a battery operated radio to get latest emergency information. |
| | If your office roof is accessible by ladder, prop it against the building so you and firefighters have access to the roof. |
| | Mark your position clearly with anything that may signal rescue workers to your presence inside the building. This could be articles of clothing or bright colored material attached to the outside of your location. |
| | Close windows, vents, doors, blinds, etc. Shut off gas meters, pilot lights and propane tanks. Turn on all lights in the building to increase visibility in heavy smoke. |

| | |
|---|--|
|  | After a Wildfire |
| | Immediately check the roof and put out any fires, sparks or embers (if accessible). |
| | If there is no power, check to make sure the main breaker is on. Fires may cause breakers to trip. If the breakers are on and power is still not available, contact the utility company. |
| | ALWAYS contact 911 if any danger is perceived upon re-entry and contact local experts before finally moving back in. |




Your Employees

| | |
|--|--|
| | Train your employees in general fire safety. This is especially important for tasks with a high fire risk, such as welding and cutting, fueling vehicles, working with flammable liquids, etc. |
| | Teach employees about the importance of good housekeeping and grounds maintenance in preventing and controlling fires. |
| | Have an adequate number of appropriate fire extinguishers and maintain them properly. |
| | Train key employees about when and how to use fire extinguishers. |
| | Consider when and how to evacuate employees if a wildfire threatens. |
| | Establish an evacuation plan and keep it up to date. |
| | Hold evacuation drills regularly so all employees will know who is in charge and so that they become familiar with evacuation routes and routines. |
| | Make sure all employees can get out of the building, find shelter and communicate with a responsible person. |
| | Plan primary and secondary exits from your buildings. Consider how employees will escape if the doors or windows are blocked by an exterior fire. |
| | Plan two evacuation routes out of your neighborhood. Consider how employees will evacuate on foot if roads are closed or impossible to use, such as being blocked by emergency personnel. |
| | Remember that ponds, lakes, rivers and landscaping or swimming pools can serve as safety zones. |
| | Keep appropriate emergency supplies on hand, including flashlights, a battery-powered portable radio, extra batteries, first-aid kit, manual can opener, non-perishable foods and bottled water. If designated employees will be working to protect the property, have appropriate clothing available, such as work boots and gloves, personal protective equipment and sturdy work clothes. |
| | Teach employees about wildfire risks and preparedness. Provide information to help employees protect their homes, too. |
| | If you are located in a wildfire area, consider advising employees to keep personal disaster supplies and copies of important documents at work in case they need to evacuate from work without being able to get home. |


CYBER SECURITY PREPAREDNESS


Cyber Security Incidents and Breaches can be very costly to a small business to include bankruptcy if data entrusted to your organization were lost, stolen, or mishandled. Impacts of Cyber Security Breaches can cost millions of dollars, lost reputation, and fines.

Below is a checklist of just some of the things to consider to prepare your business for such an event as well as to ensure the safety of the people within your organization.


| | |
|---|--|
|  | Before the Onset of a Cyber Security Incident |
| | Know what devices are connected to your network. Each computer, printer, mobile device, or other network device introduced to a network introduces risk of being compromised either by unauthorized use, mis-configuration, or lack of maintenance of security. Knowing what devices are on your network allows for inventory of those devices and control of use and security. |
| | Know what software is installed on the business systems and devices. Software can be manipulated to allow unauthorized access to a device or unauthorized software could add risk to your environment with unknown functionality. Inventory the software that is used for your organization. |
| | Know which personnel have access to your network and to what level of access. Users are the primary threat to any data due to lack of education, mistakes, or insider threat. Know your users and know what access they have to your business network. Restrict access to what they need to do their jobs and monitor access granted to sensitive data or computer systems. |
| | Know if you are using strong passwords for access to sensitive data or business applications. Password length is key. Review the password policy for the organization. Also use complexity with a password to include upper case letters, lower case letters, numbers and special characters. However, focus on using longer passwords up to 10-15 characters. Use a password manager application to prevent passwords being stored in insecure methods. Also consider using a multi factor authentication solution to augment your passwords with another layer of authentication to prevent a stolen password being used for unauthorized access to critical data systems. |
| | Once an inventory of devices and software is complete, create a baseline to protect your data and data systems by setting up computers with security in mind. The baseline will identify a starting point of known inventory of devices and software. Any changes can be quickly identified and tracked. Use the baseline to track how computers, software, and web browsers are patched with the latest updates. Install anti-malware solutions on all computers. Finally, educate your users of these topics on a regular basis - an educated user is a secure user. |

| | |
|--|--|
| | <p>A back up of critical data and data systems will help mitigate Ransomware attacks - a costly and devastating attack that renders critical data un-accessible in order to exploit money from the victim. A good back up program will save critical data and help you get your business running again quickly. Test your back up program on a regular basis to make sure it will work when needed in an emergency. Also, isolate your back up system of the network to protect it from attacks. Have a redundant back up system in case the primary back up system is unavailable. Create and rehearse a recovery plan on what needs to be done when critical data or data systems are unavailable.</p> |
|--|--|

| | |
|---|--|
|  | <h3>During the Onset of a Cyber Security Incident</h3> |
| | <p>Use your recovery plan.</p> |
| | <p>Quickly identify the compromised assets and isolate them from the network. If the compromised computer was suspected of use in criminal activity, contact the Idaho State Police.</p> |
| | <p>Document times and events of what happened in a log.</p> |
| | <p>Restore the compromised devices with back ups or by reinstalling the software. Utilize any external resources to assist, such as third-party vendors, cyber insurance, breach coaches, legal representatives or internal employees.</p> |
| | <p>Restore the device back to the network and monitor closely for any changes. Have an after-action report that explains what happened and how it was corrected. Educate your employees how to better respond in the future.</p> |


| | |
|---|---|
|  | <h3>After the Onset of a Cyber Security Incident</h3> |
| | <p>Review what worked well and what failed and refine the response program.</p> |
| | <p>Continue to monitor the device that was compromised and recovered for any changes.</p> |
| | <p>Review when critical data is backed up.</p> |
| | <p>Periodically verify that the back ups are complete.</p> |

| | |
|--|---|
| | Assess an emergency contact list for updated information. Identify roles of who will do what during the incident. |
|--|---|

| | |
|---|---|
|  | Your Employees |
| | Train your employees about general cyber security safety. A good cyber security awareness program with training modules can be implemented to help employees understand they are the front line to good cyber security. |
| | Teach employees about the importance of good housekeeping. A clean desk keeps sensitive data from being viewed by unauthorized people. |
| | Teach employees that emails should be carefully reviewed. If an email is not expected, has a sense of urgency, or it is from an unidentified entity then employees should report the email to the information technology department for review. |

EMERGENCY COMMUNICATIONS

Communication is one of the most important functions you take part in as a business. How you communicate with the general public, your customers, staff and vendors is critical to the continued success and long term viability of your operation. It is vital that you create an Emergency Communications Plan. The following checklist will help you navigate through any crisis.

| | |
|---|---|
|  | Determine Roles and Responsibilities |
| | Appoint primary decision maker/coordinator. |
| | Appoint back up decision maker(s). |
| | Outline roles and responsibilities for additional participants. |
| | Determine entities with which you communicate |
| | Employees |
| | Stakeholders |
| | Shareholders |
| | Vendors |

| | |
|-------------------------------------|--|
| | Clients/Customers |
| | Regulatory Agencies |
| | Media |
| | Other: |
| <input checked="" type="checkbox"/> | Document When to Activate Plan Using Criteria Such As: |
| | Length of time of outage/interruption. |
| | Severity of interruption. |
| | Percentage/Number of employees, departments impacted. |
| | Prolonged loss of contact with clients and/or vendors. |
| | Other: |
| <input checked="" type="checkbox"/> | Determine, document and publicize an emergency communications plan: |
| | Phone/email tree (include spouse/family information for employees). |
| | Employee evacuation plan |
| | Website emergency messaging system |
| | Phone/Voice mail emergency messaging system |
| | Plan for multiple forms of communication: text, email, voice mail, etc. |
| <input checked="" type="checkbox"/> | Educate employees about the communications plan |
| | Document in hard copy and electronic formats. |
| | Train current and new employees. |
| | Remind employees about emergency communication plan, including pocket cards, fold-out cards, brochures and booklets. |
| | Update information regularly and re-educate employees |

VENDOR ASSESSMENT

The main objective of a vendor assessment is to determine your vendors’ ability to continue service despite any sort of interruption in normal operations. This could include its ability to respond during an interruption to your organization or within its own organization. It is important to complete this assessment for each of your critical vendors so you can understand the level of risk that each poses and plan for alternatives in the event of a recovery.

(Photocopy this section and attach to work book for multiple vendors.)

Step 1: Determine who is a Critical Vendor

Complete the vendor contact information. Then answer each of the questions below to determine the level of vitality to your organization. A “Yes” to any of the statements below would classify this vendor as critical. There may also be vendors who don’t meet one of the criteria below, but could still be a critical vendor. If this is the case, put the reasons under “Special Circumstances.”

| | | | |
|------------------------------|--------|------|--|
| Vendor Name: | | | |
| Vendor Business Description: | | | |
| Contact Name: | | | |
| Contact Phone: | | | |
| Contact Email: | | | |
| Address: | | | |
| City: | State: | Zip: | |

| Question | Y/N | Notes |
|--|-----|-------|
| Access to critical company data? | | |
| Performs one or more critical functions? | | |
| Access to sensitive/confidential customer data? | | |
| Direct impact to revenue or expenses? | | |
| Directly impacts ability to perform one or more critical business functions? | | |
| This vendor is the only one who can provide this product/service? | | |

ASSESSMENT

Special Circumstances: Another reason or special situation where this vendor may be critical to business continuity.

Critical Vendor? (Y/N)

VENDOR ASSESSMENT

Step 2: Determine the Level of Risk this Vendor Poses to your Organization

Use the chart below to determine the level of acceptability and impact for your vendors in key areas on business preparedness. This should help you determine your level of risk for each critical vendor. Determine the level of “acceptability” for each statement in the second column – how acceptable is the vendor’s functionality for the “attribute” in question? You should also determine the impact of this function – how important is this attribute in the vendor’s ability to meet your needs as a customer, should that vendor experience an interruption?

Areas with Low Acceptability and High Impact pose the greatest risk while areas with Low impact and High Acceptability pose the lowest risk.

| Attribute | Impact & Acceptability | Notes |
|--|---|---|
| <i>Example: Has 24 hr. customer support</i> | Acceptability <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | <i>Vendor promises 24 hr. support by phone, low level of risk in this area.</i> |
| | Impact <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| Insurance coverage is adequate | Acceptability <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| | Impact <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| Business continuity plan in place | Acceptability <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| | Impact <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| Information security policy meets our organizational standards | Acceptability <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| | Impact <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| Remote access to this vendor | Acceptability <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| | Impact <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |

| | | |
|---|---|--|
| Free of negative publicity | Acceptability <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| | Impact <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| Will remain financially viable for the foreseeable future | Acceptability <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| | Impact <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| Has a clearly defined service level agreement with our organization | Acceptability <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| | Impact <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| Provides a guarantee for availability | Acceptability <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| | Impact <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| Contractual terms consistently met or exceeded | Acceptability <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| | Impact <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| A non-disclosure agreement is in place between parties | Acceptability <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |
| | Impact <input type="radio"/> High <input type="radio"/> Med <input type="radio"/> Low | |

ADDITIONAL INFORMATION

Websites

Idaho Office of Emergency Management - Public Private Partnerships

www.ioem.idaho.gov

Institute for Business and Home Safety: Open for Business - Valuable planning worksheets in Microsoft Word and PDF Formats allowing you to save and print your completed plan.

www.disastersafety.org

Federal Disaster Assistance and National Flood Insurance - What you need to know.

1-800-427-4661

<http://www.fema.gov/business/nfip>

<http://www.floodsmart.gov>

Ready Business: Preparedness Planning for Your Business -

www.ready.gov/business

Training

Many courses are offered at the FEMA Independent Study Program at no cost. Most of these classes take very little time. <https://training.fema.gov/is/crslist.aspx>

Some of the courses offered:

Protecting Your Home or Small Business from Disaster

<https://training.fema.gov/is/courseoverview.aspx?code=IS-394.a>

Fundamentals of Emergency Management

<https://training.fema.gov/is/courseoverview.aspx?code=IS-230.d>

Are You Ready? An In-depth Guide to Citizen Preparedness

<https://training.fema.gov/is/courseoverview.aspx?code=IS-909>

Workplace Security Awareness

<https://training.fema.gov/is/courseoverview.aspx?code=IS-906>

Public-Private Partnerships

Idaho Office of Emergency Management
(208) 258-6520 (Office)



**IDAHO OFFICE OF
EMERGENCY MANAGEMENT**

4040 West Guard Street
Building 600
Boise, Idaho 83705-5004

www.ioem.idaho.gov