



Absorb.com • 3350 Ridgelake Drive Suite 207 • Metairie, LA 70002
Phone: (504) 212 - 3000 • Fax: (504) 837 - 7988 • info@absorb.com

Small Business Disaster Preparedness / Business Continuity Plan

We've prepared this document in order to not only help you better prepare your business for a disaster but shorten your recovery time. While the points below may not fit any business perfectly, they may be used as a framework and built upon as you see fit. It's important to mention that while most, if not all, of your employees should have access to this plan, caution should be taken with more sensitive information. Weigh the cost vs. reward of cataloguing any information that could fall into the wrong hands.

After each point there is a blank for an Attachment number. For the purpose of consistency only one blank space is given where certain organizations may require more. When it becomes necessary to add additional information or take notes on a particular item simply add a supplemental page and list its reference number where applicable.

1. Create a team. While smaller businesses may be perfectly comfortable with one crisis management contact, larger organizations may require departmental or district team leaders to act as a coordinated Emergency Management Team. The first task of your crisis management team should be to discuss and collect all information necessary to complete your plan. List the team leaders for each of your locations below:

Location: _____ Team Leader: _____
Attachment #: _____

2. Identify the key threats to your business and establish a set of contingencies that best addresses them all. While common threats like hurricanes, earthquakes and fire are generally first to come to mind, there are other threats that occur less frequently and if left unaddressed can be equally damaging. These additional threats may include: power interruptions, blackouts, hazardous materials evacuations, terrorist attacks, industrial sabotage, human error, viruses, data corruption and supply shortages (remember, vendors can have disasters too). List your threats below in order of likelihood and be sure to keep them each in mind through every stage of discussion:

Threat 1: _____ Threat 2: _____
Attachment #: _____

3. List each of your company's locations and the address information for a secondary location to be used as an alternate workplace in the event of a disaster:

Location 1: _____ Alternate 1: _____

Attachment #: _____

4. Continuing operations in the face of adversity may come at a cost. In the interest of efficiency, list any products or services which may have their production or fulfillment temporarily postponed in the event of a disaster - products or services which you may deem expendable given limited production resources.

Product or Service 1: _____ Product or Service 2: _____

Attachment #: _____

5. Intellectual Capital, or the knowledge of the workings of your company, can be as important as your physical location. You must ascertain who knows what about your operations and how that knowledge can best be passed along in the event of an emergency. Adapting properly to a workforce shortage can make or break a successful crisis response. Ensure your staff members have been cross-trained and are prepared to fill other roles within your organization should the need arise. Based on your minimum staffing requirements, list key personnel or departments and secondary roles each may fill in the face of disaster.

Personnel 1: _____ Alternate Position 1: _____

Attachment #: _____

7. What means are required to bring your products or services to market: telephone, delivery vehicles, Internet or representatives? Based on the type of business interruption, can new vehicles, systems or staff be secured and if so, who from and in what period of time? If your delivery method relies on a 3rd party is there another means to acquire the same service? List each method of delivery and an alternate replacement source as well as your primary contact if applicable:

Delivery Method 1: _____ Alternate Method 1: _____

Primary Contact 1: _____ Alternate Contact 2: _____

Attachment #: _____

8. All businesses in our data-rich environment should not only have an onsite copy of their data but a secondary offsite backup as well. It is important to note, however, that traditional remote data backup providers only offer data storage. In the event of a disaster that damages your computer network, your files may be retrieved but once downloaded the majority of your files may not be accessible without their corresponding software installs and until your computer network is rebuilt to the previous specifications, many applications will fail to work without the proper paths to databases and other resources.

Absorb.com has the unique capacity to virtualize a client's entire office including all of their servers and software - their files are not only backed up, but accessible from anywhere and functional. Day-to-day operations can resume within minutes of a disaster rather than weeks or months.

If you do not have an Absorb system in place instruct employees to review all key software applications that they use to access or generate data, list them below and trace the data to its storage location. See to it that all information is backed up at regular intervals.

Software Application 1: _____ Data Location 1: _____

Is this data backed up? _____

Attachment #: _____

9. Are important physical documents stored in a fireproof / crushproof safebox? An up-to-date Document Retention Plan or DRP is critical to business continuity during a crisis. As part of a Document Retention Plan it is crucial to determine which documents, (if not all) should be scanned and added to your companies local and remote data backup sets. Below is a list of documents that may or may not apply to your organization:

EIN#, ER#, IRS Determination Letter, IRS Form 1023, current and previous Form 990s, financial statements, current and previous audited financial statements, bylaws, mission statement, board minutes and upcoming agendas, corporate seal & other Intellectual property, blank checks, employee records, client records, vendor records, receipts, equipment & location lease information, certifications and a list of computer passwords. As each relevant document is scanned and added to a backup set, list it below. There should be one easily accessible directory that contains digital copies of all of your important documents, it should be backed up and listed below.

Digital Document Location: _____ Backup Location: _____

Attachment #: _____

10. The most overlooked and least understood player in our daily manipulation of data is our software. Just as you did in item 8 above, have employees reflect on their daily manipulation of data and make note of all key software applications. Find and store each software installation disk and list both the version that was installed and the current working version. If equipment is replaced and software reinstalled, critical software updates may have to be installed in order to access data properly. Also catalogue any username, password

and vendor contact information. If possible inquire with Absorb.com about backing up entire working copies of your software systems.

Software Name and Version: _____ Location of Installation Disks: _____

Attachment #: _____

11. More than likely your company's online presence and email are managed by a third party. Make sure that the hosting and storage of this online data is located out-of-state to avoid interruption due to geographically localized disasters. Identify whether or not your email is stored at the host or downloaded to local equipment and make arrangements to archive this remotely. With damage to your physical location your online presence may have to be retooled to better interact with employees, vendors and clients. List the contacts necessary to configure it to do so and the changes you may have to make to accomplish this goal.

Emergency Online Resource: _____ Primary Contact: _____

Attachment #: _____

12. Consider strategic alliances with vendors, suppliers and dare we say ... the competition. Discuss an extension of credit with vendors should funds not be readily available, review alternate means of securing supplies if you or a supplier suffer an interruption in service and lastly if you cannot provide a valuable service to a client, carefully weigh the outcome of them not receiving it at all, verses your providing it through a competitive source. List any alliances and contingency plans below as well as appropriate contacts.

Alliance Contact: _____ Contingency Plan: _____

Attachment #: _____

13. The human factor - Facilities, computer networks and machinery are only as good as the people that operate them and those people have lives and family outside of a relationship with their employer. If you bank on having access to key employees during a widespread crisis you will lose more often than not. What an employer can do is communicate and coordinate with employees to make sure that families are included in disaster preparedness and that employees have the resources necessary to manage both their personal and occupational responsibilities. Discuss both family and professional disaster preparedness plans with your employees and develop a mutually beneficial arrangement rather than dictating.

List employee contact information as well as their emergency contact information:

Employee: _____ Emergency Contact: _____

Attachment #: _____

Insurance Provider Policy Number and other recovery information:

Attachment #: _____

Company Bank Information or Banking contact Name, Authorized Check Signers or individuals authorized to manage transfers of funds:

Attachment #: _____

Primary IT Contact: _____ Contact Information: _____

Attachment #: _____

Key Clients and their Contact Information:

Attachment #: _____

Key Vendors and their Contact Information:

Attachment #: _____

The competition:

Attachment #: _____

Additional Notes: