RED WIRE SERVICES
PO Box 46454 // Seattle, WA 98146 // T 206.829.8621 // F 206.826.1223 // info@redwireservices.com

Get Started Today: *Micro Edition*

The most important thing you can do to prepare your business is to *start today*. A complete disaster recovery plan can be an overwhelming process; however it's easy to implement a few simple changes that will make you much better prepared for a disaster. Once the basics are covered, you can build incrementally toward a more comprehensive and robust plan.

As you complete these checklists, remember that a disaster is not only a natural one (fire, earthquake, flood), a *disaster* is anything that significantly impacts your business systems and core processes: leaky pipes, equipment failures, extended power outages, employees unable to reach the office, even theft.

Step 1: If you do nothing else … ensure that:

#		YES	NO	Don't Know	Assigned To
1	All data is backed up at least on site to prevent loss from human error and equipment failure (the most likely causes of data loss).				
2	Copies of all employee, customer, and supplier contact information are stored at multiple locations easily accessed during/after an event. *Include: alternate email addresses, cell phones, and home phones.* (During a disaster situation, many communication paths may be inaccessible – it's critical for a business to maintain communications during an event.)				
3	Digital copies of important paper documents have been made (leases, tax information, contracts, insurance policies, and inventory lists). Copies are available in multiple locations that can be accessed even if primary business location is inaccessible.				
4	Each business location has disaster supplies, such as flashlights, first aid kits, emergency radio and batteries, at least three days of water and food, and tools[1].				
5	AT LEAST ANNUALLY: Review all of the above to make sure your documents are up to date. Test recoveries of all data to ensure it's there when you need it.				

[1] Find more information at http://www.ready.gov/business/

Step 2: Gauge Your Current Recoverability

#		YES	NO	Don't Know	TAKE ACTION ?
1	Can you afford to send your employees home and your customers away in the event of an extended power outage? - If no, do you have alternate power available? - If not, is it cost effective to install an alternate source of power?				
2	Are copies of your critical data stored outside of your region or at least outside of your primary building? - If no, can you afford losing all of your data if there is a local or regional disaster? - How many days can you be without data in the event of a widespread disaster?				
3	Are you following IRS and regulatory guidelines for data retention? - How long must you retain each set of data? - Do you have a working process in place to purge old information that is no longer needed? (Keeping unneeded data causes confusion and increases costs to maintain and protect data.)				
4	If a critical system failed today in your business, how long would it take for your IT staff or partner to respond? How many hours/days until things are back to normal? - If they are not available, can other members of your team recover the system or data themselves? - Are systems documented well enough that a knowledgeable third party could recover the systems if no one else is available?				

#		YES	NO	Don't Know	TAKE ACTION ?
5	If you have backups in place: - When were they last tested? - How often do tests take place? - Are you confident recovery processes will work when needed?				
6	If a key partner has a failure and is unable to provide service: - Can your business continue without them? - What is your alternative plan(s)? - How do you deal with extended phone and internet service provider outages?				
7	Is key equipment and inventory elevated above floors to avoid damage due to flooding?				
8	Do you have insurance in place to protect business assets *and income* from earthquakes, floods, fire, inaccessibility, or the untimely death or disability of key employees?				

Step 3: Gather Information for Additional Data Protection

If you've decided a more robust and comprehensive disaster prevention and recovery plan is needed for your business, answering the following questions will help get you started and bring any outside help up to speed more quickly.

1. Can you establish an estimated cost per hour or per day of system downtime for your business? Note that amount here. This will help determine which mitigating processes are cost effective for your business.

DOWNTIME COSTS	Per Hour	Per Day
Estimated total worst-case cost of system downtime for your business		

If you struggle to come up with accurate daily or hourly downtime costs for your business, start with your average yearly revenue divided by 52 weeks; this is a recommended starting budget for Disaster Recovery / Business Continuity Planning. Dividing this number by 5 will yield a daily downtime cost, by 40 an hourly cost (assuming an 8 hour work day).

Maximum Spend	Estimated Budget
$\frac{Yearly\ Revenue}{52\ weeks}$ =	

2. How many PCs, Macs, or other workstation computers does your business own? How many are laptops? Is any critical data stored *only on these devices*?

COMPUTER INVENTORY					
#	Computer Model	PC/Mac?	Laptop?	Quantity	Critical Data stored ONLY on this device?
1					
2					
3					
4					

3. What systems are currently in place to protect and recover data? Who is responsible to ensure these systems work properly during a disaster?

4. List every application your company uses that is critical to keeping your business running. Put the most critical application first, then the second most important and so on. This is your *recovery order.*

   - RTO: For each application, determine *how long your business can live without access to each application.* This is known as a Recovery Time Objective or RTO.
     Keep in mind that the lower the RTO, the more expensive it will be to meet.

   - RPO: For each application, list the *maximum amount of acceptable data loss in hours*. This is known as the Recovery Point Objective, or RPO. For example, if you decide the RPO is 12 hours, then the data from up to 12 hours before the event must be re-entered manually. As with RTO, the lower the RPO the higher the cost.

APPLICATION INVENTORY				
#	**Application**	**Critical Recovery Order**	**RTO**	**RPO**
1				
2				
3				
4				
5				
6				
7				
8				

5. List the service providers you depend on to keep your business running and identify alternate providers you could switch to quickly if there was a problem. Being able to utilize an alternate provider quickly often requires an agreement to be created *before* the disaster happens. Start by considering providers of email services, phone services, Internet connectivity, and other service partners specific to your line of business.

SERVICE PROVIDER INVENTORY				
#	**Required Service**	**Current Provider**	**Alternate Provider**	**Agreement in Place?**
1	Email			
2	Phone			
3	Internet			
4	Online Backup			
5	IT Support			
6	Website host			
7	Suppliers of raw goods			
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				