Date: 10/5/2019

Version 1.0

IT Disaster Recovery Plan Template

# 1. 0 Purpose

To provide our members a template that can be modified for your company’s use in developing an IT Disaster Recovery Plan. The IT Disaster Recovery Plan compliments your company’s cyber incident response plan, your company’s backup plan and your IT inventory. The purpose of an IT Disaster Recovery Plan is to ensure your business can respond to a disaster or other emergency that affects IT systems, with the intention of minimizing the effect on your business operations.

# 2.0 Business Process Analysis

In order to adequately plan for an event that would negatively impact your business, a business process and business impact analysis must be completed. The business process analysis is a systematic method of examining, identifying, and mapping the functional processes, workflows, activities, process owners, personnel expertise, systems, data, interdependencies, alternate locations, and resources needed to perform your company’s essential business functions.

This analysis is conducted by leveraging your company’s IT inventory. Your company’s IT inventory should list all servers, desktops, laptops, wireless devices software applications, and data. Evaluate your company’s backup policy which will identify how and what data is backed up as well as which systems should be brought online first. Identify and prioritize the critical software applications and data and the hardware required to run them.

Once complete, this section would describe the results of this analysis.

# 3.0 Business Impact Analysis

A Business Impact Analysis (BIA) is a method of identifying the potential events (fire, flood, malware) and the negative impacts as a result of your company’s inability to perform an essential function. A Business Impact Analysis assesses the operational and financial impacts of a disaster, with consideration to the time and duration of the event. The impacts lay the foundation of the BIA.

Impacts to consider include:

* Financial Impacts
	+ Lost sales and income
	+ Delayed sales or income
	+ Increased expenses (e.g., overtime labor, outsourcing, expediting costs, etc.)
	+ Regulatory fines

Date: 10/5/19

Version 1.0

IT Disaster Recovery Plan Template

* Operational Impacts
	+ Contractual penalties or loss of contractual bonuses
	+ Customer dissatisfaction or loss of customers
	+ Delay of new business plans

Include an estimate of the time and duration of the event (Wednesday morning, 10;00 AM; event lasts 72 hours). Consider the impacts of different lengths of time or that occur at during different periods of the year. A chart like the one listed below would be helpful in this section.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Process | Operational Impacts | Financial Impact | Recovery Point Objective (RPO) | Recovery Time Objective (RTO) |
| Point of Sale failure | Inability to process financial transactions;Suspension of activities;Loss of new customers | Loss of Revenue from lack of sales | <10 minutes | <10 minutes |
| Website shut down | Inability to advertise services; inability to interact with customers; customers can’t find your company | Loss of Revenue from inability to process transactions | <8 hours | <8 hours |
|  |  |  |  |  |

Recovery Point Objective (RPO) - is the age of the files that must be recovered from [backup storage](https://searchdatabackup.techtarget.com/definition/backup-storage-device) for normal operations to resume if a computer, system, or network goes down. The RPO is expressed backward in time from the instant at which the failure occurs, and can be specified in seconds, minutes, hours, or days. Your backup service provider will be able to provide this data for you - they can tell you how often your systems are backed up.

Recovery Time Objective (RTO) - is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs. Your CEO or process lead should be able to define this for your company.

**4.0 Building the Plan**

Once the analysis is complete, it is time to build the plan. The analysis will have identified your essential business functions, the order in which they need to be restored, the process owner (or cognizant lead for the process), the resources involved in the restoration, and the steps/activities involved. Your company may only have three - five essential functions so it’s important before you have an event, to document the

Date: 10/5/19

Version 1.0

function completely. This map will aid when you are in crisis mode -- you will have all the data need to efficiently restore the function. Once the essential function is described, identify the recovery method/methodology. As an example if you had a fire that damaged one of your servers, the recovery steps would include: purchasing a new server; configuring the new server (specify who will do this); reloading data and software; testing; approving the test; and placing server in full use. Using the BIA data on recovery time, you would be able to decide how long you would be without use of the data and systems on the server and when you would like to see the server back on line (Recovery Time Objective).

**5.0 Roles and Responsibilities**

The next section of the plan should delineate the roles and responsibilities involved in recovery operations. Include both your staff and third party contractors who are supporting the recovery effort. A sample chart is provided below:

|  |  |  |
| --- | --- | --- |
| Process Owner/Key Personnel | Essential Function | Role/Responsibility |
| Joe Small  | Company Management | CEO, Owner, IT Disaster Recovery Plan activator |
| Patricia Business | Website | Website Administrator |
| GoDaddy | Website | Website Hosting |
|  |  |  |
|  |  |  |

Another helpful resource is to include a listing of third party providers; their contact information; their role and reference document (contract).

|  |  |  |  |
| --- | --- | --- | --- |
| System | Vendor Contact | RPO | RTO |
| SquareCash | 1-234-567-8900 | See contract dated 01-15-2018 | See contract |
| Bob’s Electricians | 1-222-333-4444 | N/A | 48 hours |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

While this plan/template is for IT recovery, the same methodology can be used for any essential function. Ensure your backup policy and IT Disaster Recovery Plan reference important contract documents of third party vendors.

IT Disaster Recovery Plan Template

Date: 10/05/19

Version 1.0

Once the plan is built it is important to communicate to all employees their role and responsibilities in the event of disaster. An industry best practice is to conduct a table top exercise annually.

# 5.0 Plan Activation and Disaster Communications

A. Activation. The first step is to determine an event has occurred, and to activate the plan. To activate the plan, the plan administrator (i.e. CEO) is notified of a potential event, assesses the situation and determines what part or parts of the plan needs to be activated. The Plan administrator is responsible for activating the plan and for contacting the appropriate staff and support staff (may include third party contractors). The notification process continues until all members of the company have been informed of plan activation. At this time, supervisors should clearly communicate the expected actions to their subordinates (i.e. activities involving data backup, data reporting, etc.)

B. Crisis Communications. After the plan has been activated, and personnel have been notified so that recovery operations can begin, now is the time to dust off your crisis communications plan. Determine who should be notified externally and the message. As an example, if you had a fire and part of your facility was damaged, you would notify your customers and suppliers of the event; your estimate for when you might be back up and your new business location. Define both of these activities in this section of the plan.

**6.0 Recovery and Restoration**

This phase includes recovery and restoration. Include in this section guidance to the company on how the IT disaster might be addressed and what will be communicated to your staff and customers. Thinking through the recovery - how long it will take, what changes you might make and what you might want to communicate is an important step that is often overlooked. While it is difficult to plan out every possible event, documenting your expected recovery process and restoration steps will assist during a crisis. This planning step might identify shortfalls that need to be addressed, such as who to contact after hours.

**7.0 Alternative Operations and Future Considerations**

Use this section to identify alternative operational scenarios such as leveraging another site, or contractor to do the work. Other considerations might include: defining the financial limit and insurance coverage limits; rebuilding; improving on deficiencies you have put off in the past. Disasters could be turned into an operational opportunity, if so, state it in this section.

**8.0 Testing, Up Keep and Leadership Commitment**

The IT Disaster Recovery Plan should be dusted off, at least once a year to make sure the plan is still valid with your business circumstances. Have your CEO sign the document. Conduct a table top exercise once a year to test the plan and train your employees.

IT Disaster Recovery Plan Template