

## A Quick Guide to Disaster Recovery planning

### KEY ISSUES:

#### PLANNING & REVIEWS

Developing a Disaster Recovery plan **and reviewing this each year** is fundamental to ensuring your business stays in business should the worst occur.

#### SYSTEMS & DATA

Disaster Recovery planning is more than taking data back-ups. Risks need to be planned for based on the potential of losing all IT infrastructure, software, telephone systems, and paper files within an office. Planning now could be the difference between staying in business or failing to recover.

#### PREMISIS

Plans for the loss of existing business premises should be developed. Where would business be conducted and how soon after the disaster event would this happen?

#### PEOPLE

In the event of a disaster, quick communication of recovery plans to Staff, Clients, and Candidates is imperative for business confidence. With plans already developed communication can be immediate and without delay.

### Planning for business success

The thought of disasters happening to our business isn't something most of us like to dwell on. Fire, flood, or failure of IT infrastructure can, and does, however happen to businesses. If no clear Disaster Recovery strategy plans are in place, this can lead to complete business failure.

To help you develop, or review, your business' plans this guide outlines the areas you should ensure are addressed within your plans and provides practical suggestions on how you can protect your business. As they say, "**expect the best, but plan for the worse**" and make sure you protect the future of your business.

### Identifying Risks

When developing a Disaster Recovery plan, start by assessing the risks your business may run. Start from a worst case scenario, and if your plans cover this then they will also cover any less catastrophic events as well.

The worse case for a business is of course that you lose everything in an office, this would include:

#### Office premises:

Losing your office in a disaster may be something you think is extremely unlikely to happen. You of course may be right, but equally many businesses in recent years have probably thought the same until their office has been flooded by freak rainstorms, or the building did catch fire, or server became unusable.

Your first step in your Disaster Recovery planning should be to address what would happen in the scenario where your business premises are destroyed or severely damaged. Where would you be able to conduct business from if your existing offices were unusable for some time, and how quickly could you make this happen?

Short-term solutions to this could be staff working from home, or moving to temporary serviced offices. Longer term this may require a move to completely new permanent offices being considered. But, your priority (as covered later) are plans to keep your business running in the period immediately following any disaster event.



#### IT Hardware & software:

At the same time as loosing an office, you could also lose all PC's, Laptops, printers, servers etc that are within the office at the time of the disaster. For both insurance and disaster recovery planning, an itinerary should be maintained of the equipment you could lose, and plans considered on how these items would be replaced.

Items such as PC's/Laptops and printers could be sourced within a day or two, or even the same day. Set-up of these items for use is straight forward if they need to utilise only standard software such as MS Office, and/or browser software. However, specialist PC software might take a little longer to install and configure so how this would be done and by whom should be planned for.

Where Servers are concerned these can be more problematic. You need to therefore factor into your plans what the spec(s) of the server you require are, where these would be sourced, who would configure / install them (and where), and how the required software would be loaded and configured ready for use (as well as any configuration needed on PC's/Laptops)..

## A Quick Solution:

The easiest way of protecting your business is to adopt fully hosted Cloud Computing solutions. These make Disaster Recovery, as well as setting-up any new offices, immediate and without any significant business disruption or effort.

## HOSTED SOFTWARE

Internet based, fully hosted solutions for your business software mean that your systems, emails, and data are accessed through the Internet. There is no software, servers, or data on your premises to be affected by any Disaster. All you need to continue your business are PC/Laptop's for staff with a browser and Internet connection.

## HOSTED VoIP TELEPHONY

With Hosted VoIP systems your telephone exchange is hosted on the Internet. Managing numbers and extensions is performed through your browser and redirected to any other telephone instantly.

## DOCUMENT STORAGE

Documents and images etc can be stored both through your hosted software, and free services such as MS Office Live.

### Telephone systems:

As with other IT hardware, if your telephone systems run through your office you require contingency plans should you lose these systems. The use of mobile phones would be a short-term solution, but your telephone numbers are with clients, Candidates, on printed literature, on your website, and on adverts etc. Ensuring these numbers can be utilised in, or redirected to, new premises (or home) is therefore of great importance. Changing to new numbers is a large and time-consuming job and is best avoided if at all possible.

### Electronic data:

Much of the data utilised within today's business is in electronic formats. You will probably have emails, MS Office documents, scanned images, and system data from front and back-office systems. Some of this data is critical to the running of your business, some less so.

You should assess the types of data that you store and access, where this is, and the relative importance of this (including any legal obligations in maintaining data). Then check how this is currently being backed-up, how/where the back-ups are being stored (this should be off-site), and how would this be restored for use if required. However, when reviewing these plans also consider the issues you have identified concerning how you would replace IT Hardware & software. Your back-ups will be of little use unless the server / PC's with the correct software installed and configured is available first.

### Paper documents:

Although paper documents are being used less and less in business, you probably still have some of these. In a disaster to your premises these documents could be completely destroyed in a worst case scenario.

Solutions could be storage of these off-site, in fire/flood resistant cabinets, or ensuring copies of all key documents are always maintained in electronic formats (so they can be managed in the same way as other electronic data).

## Developing Recovery plans

Once you have identified where your risks are (and what is required for recovery) plans can then be developed for any eventual disaster event. The specific plans you develop should outline tasks to be conducted after a Disaster based on the priority of actions for your business operations. For example, if Sales staff could not work on finding new clients for a while this would not cause a complete failure of a business. But, if Temps could not be paid, or communications continue with Temps and Clients on their Bookings how much would this affect the business?

So, your first priority in your planning should be to prioritise the areas of your business activity that would need to be operational within different timescales.

1. **Critical business issues:** Immediately following any disaster event your first steps should be one of communication. Staff, Clients, and Candidates/Temps need to be informed of what has happened and what steps are being taken to continue business. This is where your Disaster Recovery planning will start to provide immediate benefits as plans will already be clearly laid out.

Then your plans should kick-in to ensure emails and telephones are operational without delay, and the critical aspects of managing Temps in bookings and payroll processing continue. This may initially mean staff working from home as a serviced office may be sourced but may take a little time to move in and be operational.

2. **Short-term recovery:** As soon as the first phase of recovery has progressed the next phase will be to start on recovery of your less critical systems and data. This might be getting sales activity back up and running, or your general accounts software operational for instance.
3. **Longer-term:** As long as phases 1 and 2 have progressed sufficiently quickly you should still be in business and relatively stable. Phase 3 will then be to bring things back to normality and re-establish permanent offices.

T: 0800 756 6794  
E: [info@i-businessresources.com](mailto:info@i-businessresources.com)  
W: [www.i-businessresources.com](http://www.i-businessresources.com)