BUSINESS CONTINUITY PLAN

&

DISASTER RECOVERY PLAN

TEMPLATE

EC-MSP Ltd.
Dawson House, 5 Jewry Street, London EC3N 2EX
Tel: 020 3780 7200 | Email: info@ecmsp.co.uk

For further information and additional client case studies and testimonials visit our website **https://www.ecmsp.co.uk/**

OVERVIEW AND OBJECTIVES

This template discusses the various disasters that could affect your business operations and explores the options you must consider in such circumstances. The document examines how a business could continue to operate with minimal disruption to its critical functions.

The template consists of a Business Continuity element, which focuses on:

Office Facilities **Staff** **Safety**

It also consists of a Disaster Recovery element, which focuses on:

IT Recovery **Backup Facilities** **Telecoms Recovery**

By incorporating both types of planning, the template seeks to address critical events and actions that impact staff, facilities and IT components in order to provide a holistic view of the recovery and continuity process.

In the following pages, you will find the various event types described and appropriate responses outlined. A final Plan Checklist is provided to summarise all of the considerations required to create and put into effect a comprehensive BCP and DRP strategy.

While this template can serve as starting-off point, every business has unique structures, procedures and technology considerations that make it impossible to adopt a “one-size-fits-all” approach.

For assistance with creating a custom BCP/DRP plan for your own business, contact EC-MSP on **020 3780 7200**.

TABLE OF CONTENTS

MAINTAINING DOCUMENT & VERSION CONTROL

A Business Continuity & Disaster Recovery Plan is only as effective as its last update and its last test. The document control should be assigned to a senior staff member who will be responsible for its maintenance. Whenever the document is updated, the changes should be noted as a revision and approved by the appropriate staff member. A list of key BCP/DRP contacts should also be maintained. Below are examples of these types of list.

Document Control

The maintenance and updating of this document is the responsibility of:

STAFF MEMBER	DATE APPROVED	SIGNATURE

Version Control

This should be updated whenever the plan has been modified so that changes can be tracked and monitored.

VERSION	DATE	AMENDMENTS	DETAILS	AMENDED BY
1.0		**Initial Document**	**BCP & DR Plan**	

DRP Contacts

For further information regarding this document, please contact:

	COMPANY	LANDLINE	MOBILE
Company Officer			
Other contacts			

ASSESSING YOUR CURRENT SITUATION & RISKS

Business Continuity Plans (BCPs) and **Disaster Recovery Plans** (DRPs) are tools to assist your organisation in preparing for disaster occurrences that could make some or all of your resources unavailable for a period of time.

The first step in preparing for a disaster is to take a good look at your current business and determine what you consider to be critical functions and critical hardware and software components that might be at risk. You also need to evaluate your staff in terms of their ability to effectively lead a recovery effort.

Below, therefore, are some important questions to consider the answers to...

What You Need to Know Now: Pre-DRP Questions

Location: If your main site goes down, can you continue to operate from a different site?	☐ YES ☐ NO
Communications: Do you have contact information for all staff members, vendors, suppliers, IT firm, insurance companies, and any other "need to know" contacts in the event of a disaster?	☐ YES ☐ NO
Hardware: Do you know what sits on each of your servers (internet, email, printing, backup, remote access, etc.) and do you have this documented?	☐ YES ☐ NO
Software: What software and what versions of that software do you have and are these documented somewhere?	☐ YES ☐ NO
Phone system: Have you contacted your phone service provider and established a mobile phone number to be put on standby for potential redirection of your main number when and if needed?	☐ YES ☐ NO
Paperwork: Is all of your paperwork backed up, scanned or protected somehow?	☐ YES ☐ NO
Recovery information and instructions: Is your BCP/DRP stored online and accessible from a remote location?	☐ YES ☐ NO
Backup systems: Is your business data backed up and recoverable?	☐ YES ☐ NO

How a Disaster Will Affect Your Business

There are many possible disaster scenarios which can cause a wide variety of business disruptions. These disruptions can range from a component failure to a large-scale catastrophe. To make disaster planning more manageable, we have grouped these possible situations into categories, based on similar actions that will be required.

Disasters come in varying forms. We group them as follows:

TYPE 1: File loss, partial system failure, phone system failure, internet failure

TYPE 2: Loss of location but the system is not affected (most pressing threat in UK at present)

TYPE 3: Full loss of system but the location is not affected e.g. Virus, equipment theft, hacking, or power outage

TYPE 4: Full loss of location and system

TYPE 5: Loss of staff (e.g. Wholesale headhunting, lotto syndicate, bird flu etc.)

For the purposes of this document, we will focus on a recovery from a Full Loss of Location and System (Type 4), which encompasses recovery from all other event types except Type 5, which is addressed in the Staff Training & Recovery section towards the end of the document.

RESPONSE/RECOVERY TIMELINES
FOR EVENT TYPES

Just like a government official declares a "state of emergency," your company officer must decide when to call for disaster recovery actions. He or she must decide whether and when a BCP/DRP must be executed. It is important to set a fixed worst-case scenario timeframe for response and recovery. Critical Information may be unavailable (like when access to the building might be restored). Once you decide a DR event is occurring, you should move ahead with the BCP/DRP. Time is critical. From the start of action, a fully-working office can be 48-72 hours away.

Occurrence of the event: What type of event is occurring and what is the timescale to action for that event?

1. **Type 1:** File loss, system failure, phone system failure, internet failure, hardware failure
   Action: Contact IT Support Provider
   Response/recovery time: Determined by IT support
2. **Type 2:** Loss of location but the system is not affected
   Action: Relocate staff to home or second location
   Response/recovery time: Refer to BCP
3. **Type 3:** Loss of systems but the location is not affected
   Action: Full DR implementation
   Response/recovery time: Determined by IT support
4. **Type 4:** Full loss of site and system
   Action: Full DR & BCP Implementation
   Response/recovery time: Determined by IT / BCP
5. **Type 5:** Loss of staff e.g. wholesale headhunting, Lotto syndicate, Bird Flu etc.
   Action: Engage Recruitment Agency
   Response/recovery time: Varies with availability

DETAILED REVIEW
OF DISASTER EVENT TYPES

DR actions and timeframes are dependent on the type of disaster event. Once an event is defined as a disaster, recovery actions start as soon as possible, but complications and delays may impede recovery, so full recovery may take some time.

DRPs and BCPs should be designed to handle the majority of disasters that can be anticipated, but as with any serious and unexpected interruption, there can be special situations that need to be dealt with. Below are the actions, timeframes and special circumstances associated with typical disaster types.

TYPE 1 EVENT

Failure type:	There is a file loss, partial system failure, phone failure, or internet failure.
Action:	Communicate with IT for regular IT support.
Time to action start:	Immediate – establish quickest time frame to action with your IT support provider.
Special circumstance:	If a fix is not possible within 2 days for business critical system loss, change event to a Type 3 event

TYPE 2 EVENT

Failure type:	There is a loss of location but the system is not affected – (most pressing threat in the UK at present).
Action:	Relocate staff to backup location or home.
Time to action start:	1) If your location is lost for more than 1 day (unless full staff remote access is implemented), then action is immediate. 2) If police or emergency services estimate that the location will be unavailable for 1 day or longer, then action is immediate.
Special circumstance:	If, during a Type 2 event, the power is cut or systems such as internet or phones fail, then change to Type 4 event.

TYPE 3 EVENT

Failure type:	There is a complete loss of the system but the location is not affected (e.g. Virus, equipment, theft, hacking, or power loss).
Action:	Full DR implementation.
Time to action start:	Immediate – establish quickest timeframe to action with your IT support provider.
Special circumstance:	1) If any of the critical systems cannot be repaired onsite or if the time to repair is expected to be longer than 1 day, then change to a Type 4 event. 2) In this event, a loss of power will be a Type 4 event unless a generator has been agreed to. 3) Wholesale location theft results in a Type 4 event.

TYPE 4 EVENT

Failure type:	There is a complete loss of location and systems.
Action:	Full DR & BCP Implementation.
Time to action start:	1 day.
Special circumstance:	It is at the Managing Director's discretion whether action is delayed until agreement is reached with the insurance provider.

TYPE 4A EVENT

Failure type:	There is a fire, flood or similar catastrophe that wipes out everything with no possibility of location or systems being recovered.
Action:	Full DR & BCP Implementation.
Time to action start:	Immediate.
Special circumstance:	If there is no possibility of recovering location and repairing physical systems, contact your IT service provider.

TYPE 5 EVENT

Failure type:	Loss of staff e.g. Wholesale headhunting, Lotto syndicate, Bird Flu etc.
Action:	Contact Recruitment Agency.
Time to action start:	Immediate.
Special circumstance:	For bigger pandemic type events it may be very difficult to action any plans if human movement is restricted.

STAFF ACTION POINTS

Disaster events can create confusion, panic, misinformation and misdirection. In such situations, people need to be informed of what has happened and instructed on what needs to happen, with each member of staff knowing his or her role in advance. A clear line of communication should therefore be established to reach all affected parties, including internal and external organisations. A list of key company contacts should also be stored and updated on a regular basis so they are immediately available should a disaster occur.

Examples of Contact Information to be Stored and Updated

- **Full and updated staff member contact list**
- **Office management contacts**
  e.g. Services (gas, electricity, air-conditioning etc.), building services (landlord, local council., emergency services (also include disaster event numbers)
- **Full and updated customer list:**
  this should be reviewed and revised accordingly once a month
- **Full and updated supplier list:**
  this should be reviewed and revised accordingly once a month
- **Full and updated contractor list:**
  this should be reviewed and revised accordingly once a month

Examples of Actions to be Taken by Staff Members at Time of Disaster Event

Note: You need to read your own BCP/DRP, decide the event and severity, and initiate the contact of staff and all other contacts as appropriate to your business. Here are some examples of "Communication Action Branches" which could be assigned to different staff members:

STAFF MEMBER 1

- Refer to BCP plan and decide on event type and severity. Initiate staff contact.
- Engage IT support - Call IT support provider who will proceed to action DRP dependent on event type and severity.
- Get in touch with **critical** contacts and inform them of the incident and estimated lead time for recovery.
- Contact insurance company and inform of the event, confirming relevant coverage and any actions required to ensure all possible claims are covered.

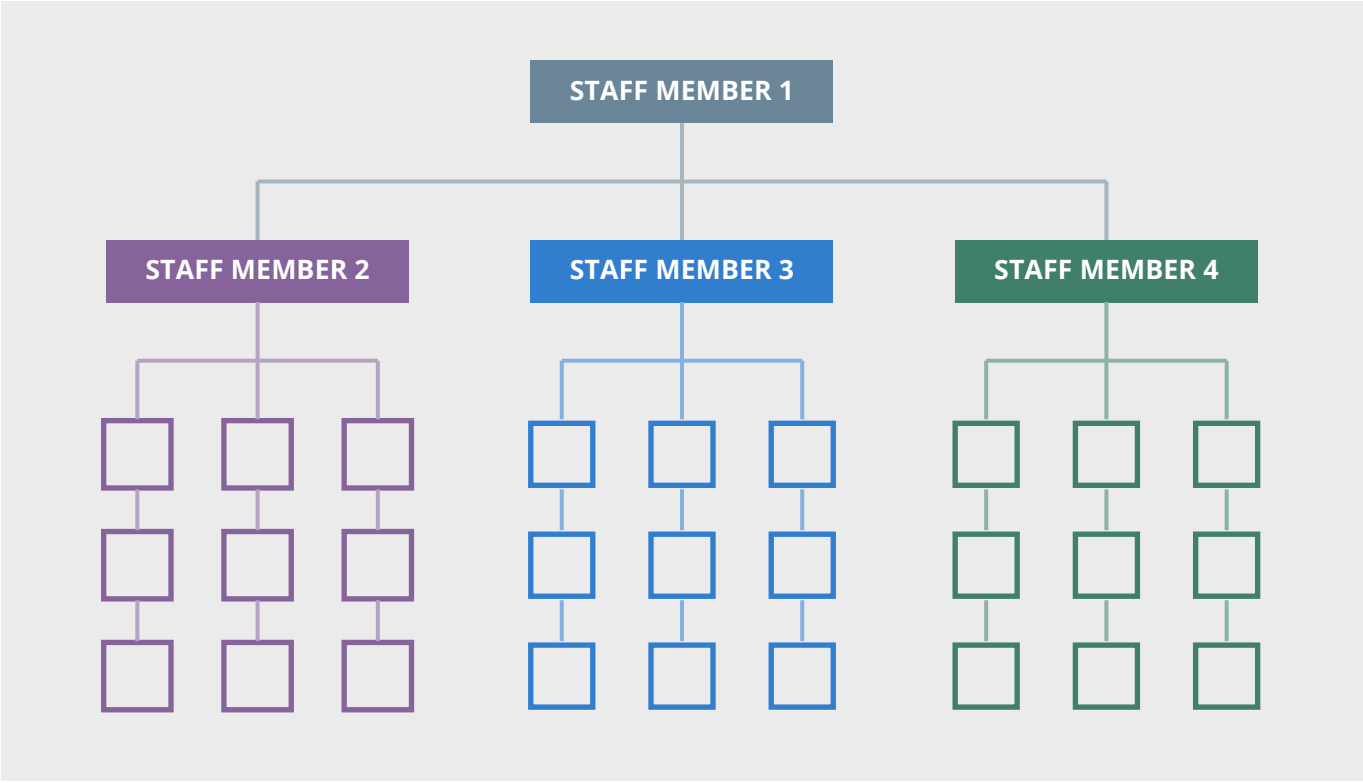
STAFF MEMBER 2

- Contact relevant staff members under your Action Communication Branch (below) and pass on the message detailing the event type.
- For location loss, contact and arrange office space for the staff on a day by day basis, and verify that the insurance company agrees with this arrangement.
- Contact any live location contractors (refer to relevant Contact List for contact information).

STAFF MEMBER 3	• Contact current clients and advise of the event type and severity along with any deadlines in the sales process that may not be met. • Contact relevant staff members under your Contact Tree Branch (below) and pass on the message detailing the event type.
STAFF MEMBER 4	• Contact Suppliers (refer to relevant Contact List for contact information) and inform them of the event type and severity along with any critical payments that may be delayed. • Contact relevant staff members under your Contact Tree Branch (below) and pass on the message detailing the event type.

Communicating The Disaster Event: The Contact Tree

The most efficient way to contact all staff members is to have a "Communications Contact Tree" in place. This enables one staff member to contact several other staff members, and if needed, those staff members can continue the chain.



BCP — LOCATION RECOVERY

Working space can be at a premium if a major event occurs. The inability to hold staff meetings and have ongoing staff interaction can severely impede business continuity. Here are three options to deal with loss of location in the disaster event stage.

a) If space is available at a Director's home, this would be preferable to rental space for the short term.	**b)** Provision space in serviced offices; locate 3 spaces in your area and ensure you have relevant contact details.	**c)** Recreate your servers in a hosted environment (for example, your IT support provider's offices) and have all staff work done remotely from home. This solution will require an investment in standby hosting space and possibly staff equipment.
Action: Identify location and space if feasible	**Action:** Confirm location and enter initial dialog with preferred location and provider	**Action:** Engage hosting facility provider

Paperwork and Non-IT Physical Items

When planning for Business Continuity, it is important to take stock all of the non-IT items that support or are a part of your business. Things like furniture items for insurance reporting, or security devices for logging into your bank, should not be taken for granted.

You may also have a lot of information on paper. Does it need to be scanned? Do you have digital backup that can be accessed remotely? It is advisable to have a process within your company for scanning all paperwork and storing it in the Cloud.

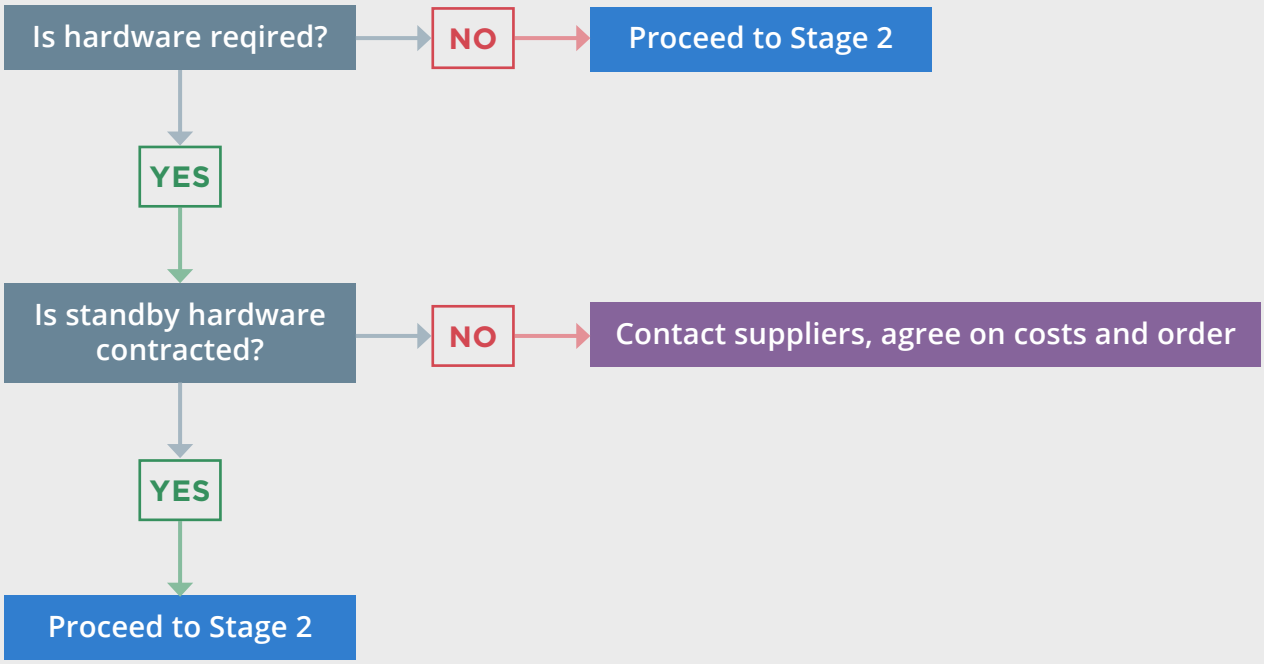
While this should be sufficient for most paperwork, there may be certain kinds (such as drawings or plans) that would be hard to digitize and almost impossible to recreate without significant effort. These, along with sensitive information like banking figures, should be stored offsite in the home of a responsible staff member.

DR — IT RECOVERY

A full IT and network recovery relies on information and backed up data kept away from the office. It is highly recommended that a full Disaster Recovery rehearsal is carried out at least once (but preferably twice) a year to ensure all relevant information and data is correct and recoverable. If this is not done, there is a significant chance that the recovery will suffer partial or total failure.

Once an event has been declared, the first point is to define the hardware requirement. Certain events will not need hardware e.g. Hacking or virus attacks that format the system.

Stage 1 – Hardware Requirements



Stage 2 – Component Recovery

The recovery of IT components can be a very daunting task, even for seasoned IT professionals on staff. This task is more easily accomplished by having an established IT provider to partner with.

EXTERNAL MAIL CONTROL	**Process:** Check with your ISP/provider to verify continued viability. If you are using an internal server, log on to the Cloud portal and use your email that way. Follow with testing.
INTERNET PROVISION	**Process:** Liaise with relevant ISP/provider to ensure at least a viable connection for your requirements. Follow with testing.

PHONE SYSTEM

Process at point of failure:

1. Contact your phone line provider and redirect main numbers to the standby mobile number you set up in the pre-DR stage.
2. Arrange for temporary lines (this may be in serviced office or at Director's location). This is only to be actioned if a significant long-term event has occurred, as line provision will take 10 days minimum.
3. Contact VOIP provider and set up a temporary VOIP provision. Consider forwarding numbers to that system.
4. Test phone system functions, including inbound, outbound, voicemail, Caller Line Identification, call forwarding and hunt groups.

SERVERS

Process at point of failure:

1. When a disaster occurs and the servers are gone, where is the data? Call your IT support or backup vendor (or obtain an offsite physical backup) and request a high priority copy to a USB drive. Provide delivery address and confirm ETA.
2. If no remote active directory exists, then provision exchange server recovery software. You should know how to back up your servers, be able to test, and have data ready to be recovered.

After Server hardware provision (Stage One):

This process is divided into two stages. The primary reason for this is to enable the flow of email as quickly as possible. Should this not be required (often provisioning of internet services is delayed), then this will all happen as one stage.

Email functionality enabled:

1. Rebuild the server, configure all users and applications; configure any printers. Test to make sure all clients have server access.
2. Test internal and external email; make sure all applications are working; test printers.

Each server needs to be tested for functionality by the relevant department.

Data recovery:

1. Recover all file data and email data (may require loss of the system while this is happening).
2. Confirm and configure any permission requirements.
3. Confirm and recover any third-party applications.
4. Test different application types and data locations on data drive; confirm emails are accurate and complete; confirm permissions are correct; test third party apps.

WORK-STATIONS & PRINTER

To reestablish business continuity, it may be necessary for staff members to work from home or from another location. Laptops can be provided to members to allow them mobility and to give you more options in staff placement. Verify that laptops are covered by insurance and, if the location is unsecured, take precautions to prevent theft.

After provisioning:

1. Build standard configuration for laptops.
2. Connect to network; test user-specific settings (email, drives, printer, etc.)
3. Give users instructions for passwords and access.
4. Test email and printing to and from multiple locations/ laptops.
5. Confirm access to all file and email data.

STAFF TRAINING AND RECOVERY

It is a good idea to assess the skill and knowledge levels of key employees and do cross-training where appropriate to facilitate recovery efforts. Periodic testing of the DRP will reveal training needs. Key staff should also be made be familiar with critical server operation, software versions, phone and telecommunications equipment, and vendor information.

It is recommended that you set up a relationship with a Recruitment Agency that focuses in your field. Creating detailed job descriptions will ensure that in the event of wholesale staff loss (a Type 5 event), you have your full requirements on hand to source new people. Reduce the risk as much as possible by backing up on the server all data that your staff might retain on external equipment.

BCP AND DRP CHECKLIST

Below is a practical checklist you can use to ensure you are accounting for the key Business Continuity and Disaster Recovery issues we have discussed in this document:

- ☐ **Document & Version**
  - Date of latest update
  - Document control manager / contacts
- ☐ **Testing**
  - Annual Test Schedule
  - Current Test Date
- ☐ **Staff Action Points**
- ☐ **Staff Communication Tree**
- ☐ **Contact Lists**
  - Staff, including job descriptions
  - Customers
  - Suppliers
  - Partners
  - Recruitment Agency
- ☐ **Location(s)**
  - Backup location
- ☐ **Paperwork & Non-IT Items**
  - Accounting & Payroll items
  - Furniture
  - Drawings & blueprints
  - Other critical paperwork
- ☐ **Hardware**
  - Servers
  - PCs
  - Laptops
  - Printers
  - Offsite Data Backup & DR Solution
- ☐ **Software**
  - Operating System and Version
  - Applications
  - Offsite Data Backup & DR Solution
- ☐ **Telecommunications**
  - Phone System
  - Intranet/Internal network
  - Internet ISP
  - Email
  - Remote access

FINAL WORD

In Business, There Should Be No Surprises...

According to the Department of Trade & Industry, 70% of companies that encounter a significant loss of data go out of business within a year. When things don't go as expected, therefore, events with highly negative consequences - whether natural or man-made - can not only interrupt business continuity, but could put an end to your business altogether. In spite of all this, in the race for market share, growth and profitability, Business Continuity & Disaster Recovery considerations still frequently fall by the wayside.

The best form of protection is to begin preparing for any such emergency today. Having a reputable and proven BCP and DRP services provider like EC-MSP is the best way to make sure you have thought through all of the myriad disaster scenarios and consequences along with their required recovery actions and timelines.

EC-MSP will work with you to ensure you have fully-established BCP & DR capabilities, along with a comprehensive and testable plan for recovering all of your vital business assets, so that in the case of your company, there will be no surprises.

Contact EC-MSP today on **020 3780 7200** to learn how we can help.

> *"Thanks to EC-MSP, we now have a robust, cost-effective solution, and trust that our data, the core of our business, is in safe hands."*
>
> **Ewan Silver**
> Chief Technology Officer, Nutmeg

> *"We view EC-MSP as part of the team. They are technically competent, extremely thorough and their engineers are easy to work with – in fact, the users at Nutmeg don't have a bad word to say about them."*
>
> **Matthew Dixon**
> Hudson Walker International

> *"EC-MSP was recommended to us and they have lived up to all expectations. The financing deal they came up with was also very attractive – ideal for a small business."*
>
> **Steve Vaudrey**
> The Clarion Agency