Business Logo Here

BUSINESS CONTINUITY PLAN

FOR SMALL TO MEDIUM SIZED BUSINESSES

DATE : ???
VERSION: ??

PRODUCED BY DURHAM CIVIL CONTINGENCIES UNIT

BUSINESS CONTINUITY PLAN

LIST OF CONTENTS

RECORD OF AMENDMENTS

Amdt No	Date	Paragraphs/Pages Amended	Initials

DISTRIBUTION

1. DISCLAIMER

This guide and template has been produced by Durham Civil Contingencies Unit to provide general information and advice about developing business continuity plans for small to medium sized businesses or voluntary organisations. It is not intended to provide detailed or specific advice to individuals or their businesses. If required you should seek professional advice to help develop an individual plan for your business. Durham Civil Contingencies Unit will accept no liability arising from the use of this document.

2. AIM

The aim of this plan is to provide a reference tool for the actions required during or immediately following an emergency or incident that threatens to disrupt normal business activities.

An **emergency** is an actual or impending situation that may cause injury, loss of life, destruction of property, or cause the interference, loss or disruption of an organisation's normal business operations to such an extent it poses a threat.

An **incident** is any event that may be, or may lead to, a business interruption, disruption, loss and/or crisis.

The plan will help to ensure the continuation of business critical services by minimising the impact of any damage to staff, premises, equipment or records.

The plan will help to include an adequate level of detail used to maintain the business and:

- To ensure a prepared approach to an emergency/incident.
- To facilitate an organised and co-ordinated response to an emergency/incident.
- To provide an agreed framework within which people can work in a concerted manner to solve problems caused by an emergency/incident.

The plan will also help to identify actions that could be taken in advance of an emergency or incident to reduce the risk of it happening.

3. BUSINESS CRITICAL PROCESSES

Whilst most parts of any business are considered important, if an incident did occur, priority must be given to the restoration of the processes that are deemed to be business critical to the performance of the company.

Business critical processes can be defined as:

"critical operational or support activities without which the business would rapidly be unable to achieve its objectives"

These individual processes must be given preferential access to premises, staff, equipment or records if an emergency situation restricted their overall availability. It is for these processes that plans need to be prepared.

4. SCOPE OF THE PLAN

The plan will illustrate how the business can reduce the potential impact of an incident by being prepared to maintain services in the event of the:

- Loss of key premises
- Loss of key staff
- Loss of IT / data
- Loss of telecommunications
- Loss of hard data / paper records
- Loss of utilities (electricity, water, gas)
- Loss of a key partner or supplier
- Disruption due to industrial action
- Disruption due to severe weather

5. ASSUMPTIONS

Generally used assumptions

- The business continuity plan will cover three scenarios: for the first 24 hours following an incident and for both 2 - 7 days and 8 – 14 days following an incident. (Recovery plans needed to cover longer periods would normally be developed during the first fourteen days of an incident.)
- The business continuity plan will be reviewed regularly, with a full update on an annual basis or where a significant change to the business occurs.

Detailed Planning Assumptions

The following assumptions have been taken into account when developing the plan:

- In the event of a major incident existing business premises would be out of use for more than 7 days.
- In the event of a less significant disruption some of the existing premises would remain in use.
- Where a generator is not available loss of electricity supply across a region could last for up to 3 days.

- The mains water supplies and sewerage services may be interrupted for up to 3 days.

- Availability of the IT network historically runs at over %. In the event of a partial failure of a server the network could be unavailable for up to hours.

- If the server suite were to be completely lost it could take up to days to restore a limited desktop service (Microsoft package, E-mail and Internet access). Other software could take even longer to restore.

- Availability of the internal telephone network historically runs at %. In the event of a failure of the iSDX there could be loss of service for up to hours.

- Access to the public telephone network and mobile communications could be lost for up to 3 days.

- In a pandemic 25% - 30% of staff could be off work at any one time. This will include those who are sick, those caring for others and the 'worried well' who are simply too scared to come to work. On average people will be absent for 5-8 days, but some may never return.

- In a fuel crisis only staff involved with delivering critical services are likely to have priority access to fuel.

6. THE PLAN

- **Form A – Immediate Actions Checklist** is a list of the actions that should be taken in response to the initial incident. The checklist is not prescriptive, exclusive or prioritised; any incident will require a dynamic assessment of issues and actions required. Depending on the scale of the incident actions can be delegated to a support team but the Senior Manager is responsible for the actions taken.

- **Form B – Response Actions Checklist** is a list of the actions that should be taken for the company to maintain business critical processes. The checklist is not prescriptive, exclusive or prioritised; any incident will require a dynamic assessment of issues and actions required. Depending on the scale of the incident actions can be delegated to a support team but the Senior Manager is responsible for the actions taken.

- **Form C – Essential Services** is a list of the essential functions undertaken by the business that must be maintained or quickly restored in the event of a disruptive incident.

- **Form D – Summary of Post Incident Resources & Equipment** summarises the accommodation and equipment needed to maintain operations.

- **Form E – Summary of Essential IT Systems & Records** summarises the basic desktop, software and systems data that need to be restored.

- **Form F – Staff Details** lists all service staff, indicating those business critical staff that will be required to maintain services in the event of an incident.

- **Form G – Key Contacts** a list of those people that would need to be contacted in the event of an incident. This could be business partners or suppliers.

- **Form H – Plan Summary** provides a single sheet summary of the main business continuity options of the plan.

Form A – Immediate Action Checklist

To be completed by the Senior Employee at the incident site

Action	Notes	Tick Done
If necessary: • Follow Evacuation Procedures • Call emergency services	• •	• •
Maintain a record of all emergency actions taken. Use the log in the Annex 6.4		
Assess the situation and level of response required. Can it be dealt with as a day-to-day management issue or does the business continuity plan need to be invoked?		
Communications: • Advise staff of the immediate implications for them and service provision • Advise staff of the immediate requirements to deal with situation, including temporary accommodation etc if required. • If necessary, advise key partners / suppliers. • If necessary speak to the local press.	• • • •	• • • •
If necessary, allow all staff to contact home to advise they are safe?		
If necessary arrange for the premises to be secured?		
If necessary, use signage to advise the move to a temporary location.		

Name of attending Senior Employee……..

Form B – Response Actions Checklist

To be completed by the Senior Employee at the incident site

Action	Notes	Tick Done
Once you are in control of the initial emergency update staff on a regular basis and keep them fully informed of developments. Make sure members of staff not directly involved in the incident, or those who are absent are also kept advised of developments. Refer to Form F or other staff listings.		
If necessary form a team of people to assist with the tasks required to restore services. These people should ideally be identified and trained prior to the incident.		
Priority should be given to the needs of the business critical processes.		
Advise all staff and key contacts (see Form G) of temporary location & any temporary telephone numbers to be used until numbers can be diverted.		
If mobile phones are being used make sure there are sufficient chargers available.		
Temporary Accommodation • Is the available accommodation sufficient for the needs of all the business critical processes or is additional alternative space required? • Do you need to arrange for replacement equipment to be ordered? • Do you have access to all essential systems or records? • Make arrangements for telephones and post to be re-directed to your new location.	• • • •	• • • •
Working at home and Non-Business Critical Staff • If available space is at a premium consider allowing suitable individuals to work from home • Non-essential staff should be sent home or reallocated to support business critical processes. • Make sure those sent home are aware of when to make contact to check on progress or when to return to work.	• • •	• • •
Create any new operational procedures and instructions.		

Give careful consideration to staffing levels. In a low staff level situation a priority will be a rota of replacements to avoid fatigue.		
Closely monitor staff issues, morale, overtime, welfare, etc. Do any of the staff need counselling?		
Do you need to complete an Accident Log?		
When ready, inform other organisations, public, suppliers, etc of resumption of normal service / contact details.		
Financial Procedures • Decide who can authorise additional expenditure • Keep records of all expenditure	• •	• •
Cancel or delegate any unnecessary meetings not connected to the incident		
Preservation of records • Do not destroy anything. Try to recover as many documents as possible and preserve them somewhere where they can be retrieved easily. This is an ongoing obligation throughout and after the incident. • Make someone responsible for co-ordinating and preserving a Master Log. • Make a record of all meetings and briefing sessions. • Make a hard copy of any relevant computer data and electronic mail.	• • • •	• • • •
Support the post-incident evaluation by direct contribution and by facilitating the involvement of key members of staff. Recovery should always be treated as an opportunity to improve the business.		
At the end of the recovery phase when normality is achieved, inform all interested parties and mark with an occasion.		
Review the Business Continuity Plan to learn from the decisions taken.		

Name of attending Senior Employee……

Form C – Essential Processes

What are the essential parts of the business that are required within the first 24 hours?

What are the essential parts of the business that are required within 2 – 7 days?

What are the essential parts of the business that are required within 8 – 14 days?

Which external suppliers / partners / contractors (if any) are dependent on the services provided by your business?

Which external suppliers / partners / contractors (if any) does your business depend upon?

Form D – Summary of Post Incident Resources & Equipment

(Excluding IT as these should be given on Form E)

Requirement	Within 24 hrs	2 – 7 Days	8 – 14 Days
People			
Number of staff (FTE)			
Furniture			
Chairs			
Desks			
Filing cabinets			
Equipment			
Office Phones			
Mobile Phones			
Desktop PC			
Laptop PC			
Printers			
Fax			
Scanner			
Photocopier			
Records			
Paper records/files			
Special Provisions			
Confidential area			
Secure area for safe			
Delivery area / Mailroom			
Air conditioning			
Storage space			
Waiting Room			
Public Access			
Wheelchair Access			

Form E – Essential IT Systems & Records

Requirement	Within 24 hrs	2 – 7 Days	8 – 14 Days
Desktop			
Microsoft Office			
E-mail			
Internet Access			
Additional Software			
Essential Computer data			

Form F – Staff Details

If an alternative list exists add details about who has access and where both paper and electronic versions are held. This avoids having to keep more than one listing updated.

NAME	POSITION/ROLE	KEY	ADDRESS	HOME	MOBILE

Form G – Key Contacts

If an alternative list exists add details about who has access and where both paper and electronic versions are held. This avoids having to keep more than one listing updated.

NAME	POSITION/ROLE	E-MAIL ADDRESS & OR BUSINESS PHONE	HOME	MOBILE

Form H – Plan Summary

Identified Risk	Recovery Option	Evaluation Criteria	Possible Further Action
Loss of Accommodation			
Loss of Staff			
Loss of IT / Data			
Loss of Telecommunications			
Loss of Hard Data / Paper Records			
Loss of Mains Services (Electricity, Water and Gas)			

Identified Risk	Recovery Option	Evaluation Criteria	Possible Further Action
Loss of a Key Partner / Supplier			
Disruption due to industrial action e.g. fuel shortage			
Severe Weather			

7. ANNEX

7.1 Assessing the risks

Use this table to produce an assessment of the current risks to your business and/or location.

Likelihood	**Impact**
Low	Low
Medium	Medium
High	High

Risk	Likelihood	Impact	General Control Measures	Possible Further Action
Fire completely destroying all of part of the premises				
Theft of computer or office equipment				
Loss of staff (Pandemic)				
Loss of staff (Serious incident / accident)				
Loss or corruption of IT data				
Loss of telecommunications				

Risk	Likelihood	Impact	General Control Measures	Possible Further Action
Loss of Electricity				
Loss of Water				
Loss of Gas				
Flooding				
Storm Damage				
Fuel Shortage				
Vandalism				
Terrorist threat				
External factor preventing access to premises e.g. fire, police incident, traffic accident				
Loss of a key partner or supplier				

Risk	Likelihood	Impact	General Control Measures	Possible Further Action
Disruption due to industrial action				
Disruption to the transport network				

7.2 Company Mobile Phone Users

7.3 Laptop users

7.4 Staff able to work from home

7.5 Emergency Operations Log

Incident:	**Date:**	**Sheet ….. of …..**

Time	**Event**	**Action**

If necessary continue on a separate sheet

8. TRAINING & REVIEW DATES

The plan will next be tested in

The plan will next be reviewed in or earlier in the event of a significant change to the business.

END