



# **BUSINESS CONTINUITY PLAN**

## **A GUIDE TO PREPARING A PLAN FOR SMALL TO MEDIUM SIZED BUSINESSES**

**PREPARED BY DEVON COUNTY COUNCIL EMERGENCY  
PLANNING SERVICE**

## CONTENTS

1. DISCLAIMER .....	3
2. BACKGROUND .....	3
3. METHODOLOGY .....	3
4. GENERAL ASSUMPTIONS.....	4
5. INSTRUCTIONS.....	5
<b>5.1 Service Impact Analysis</b> .....	6
<b>5.2 Risk Assessment</b> .....	7
6. OUTLINE RECOVERY STRATEGIES.....	11
<b>6.1 Loss of Building / Accommodation</b> .....	11
<b>6.2 Loss of Staff</b> .....	12
<b>6.3 Loss of IT services</b> .....	13
<b>6.4 Loss of telephone landline services</b> .....	13
<b>6.5 Loss of hard data / paper records</b> .....	13
<b>6.6 Loss of utilities</b> .....	14
<b>6.7 Disruption by industrial action</b> .....	14
<b>6.8 Loss of a key partner or supplier</b> .....	14
<b>6.9 Severe Weather</b> .....	14
7. FINANCIAL ISSUES .....	15
8. MEDIA COMMUNICATIONS.....	15
9. RESPONDING TO AN INCIDENT .....	15
<b>9.1 Initial Response</b> .....	15
<b>9.2 Invoking the plan</b> .....	15
<b>9.3 Action Checklists</b> .....	15
10. COLLECTING THE BASIC INFORMATION .....	16
11. TESTING AND REVIEWING THE PLAN.....	16
12. POPULATING THE TEMPLATES .....	18
<b>Form A – Immediate Actions Checklist</b> .....	18
<b>Form B – Response Actions Checklist</b> .....	18
<b>Form C – Essential Services</b> .....	18
<b>Form D – Summary of Post Incident Resources &amp; Equipment</b> .....	19
<b>Form E – Summary of Essential IT Systems &amp; Records</b> .....	20
<b>Form F – Staff Details</b> .....	21
<b>Form G – Key Contacts</b> .....	22
<b>Form H – Summary of the Business Continuity Options</b> .....	23
13. ANNEX.....	25

## RECORD OF AMENDMENTS

Amdt No	Date	Paragraphs/Pages Amended	Initials

## **1. DISCLAIMER**

**This guide and template has been produced by Devon County Council to provide general information and advice about developing business continuity plans for small to medium sized businesses and voluntary organisations. It is not intended to provide detailed or specific advice to individuals or their businesses.**

**If necessary you should seek professional advice to assist you in developing an individual plan. Devon County Council will accept no liability arising from the use of this document.**

## **2. BACKGROUND**

The requirement for Devon County Council to promote business continuity advice to the business and voluntary sectors was introduced under the Civil Contingencies Act 2004. Specifically the Act requires local authorities to provide advice and assistance to those undertaking commercial activities and to voluntary organisations in relation to business continuity planning in the event of emergencies.

Business continuity planning is seen as a way of building 'community resilience', a way of helping local organisations to help themselves, to reduce the economic impact of emergencies and to reduce reliance on public sector bodies. The result will be stronger links with the business community and improvements in the local authorities own emergency management arrangements.

The role of the local authorities in business continuity planning is as a catalyst, to raise awareness in the public and to be a conduit for information for all interested parties. The Authority is not expected to be an expert in this field, but is expected to join up with other initiatives – e.g. town centre evacuation plans – and make this pertinent for local organisations.

If you do not feel able to devote the necessary time, or you lack the expertise to complete a plan you should consider bringing in consultants to help you develop a plan specifically for your organisation.

## **3. METHODOLOGY**

The suggested methodology for producing a plan is:

- **Understand your business** by deciding which parts of the business are crucial in keeping it going. This doesn't mean that the other elements are superfluous, it just means that in a period of disruption when resources might be limited that they need to be concentrated in the areas where they have the greatest impact.

- **Access the risks** by deciding how likely an event is to occur and what the impact might be to the business. This exercise will often identify actions that can be taken to reduce the risk happening in the first place.
- **Develop a strategy and plan** based on your knowledge of the company and the risks involved. You might be willing to accept some risks but for others you need to make contingency plans. Use the templates in the accompanying document to develop a plan.
- **Test and review the plan.** All staff must understand their role in the plan. Make sure the plan is tested and updated regularly. It is pointless having an out of date plan gathering dust on a shelf.

#### **4. GENERAL ASSUMPTIONS**

When determining your strategy you will need to make certain assumptions about the type of business interruption you might experience. For example:

- In the event of a minor disruption assume existing accommodation would be out of use for 24 hours. For a more significant disruption assume access would be denied for more than 7 days.
- How robust is your IT system? Do you have maintenance contracts in place, if so how long might you have to wait for the systems to be restored? Assume you will not have access for at least a day, longer in the event of a major IT incident.
- How reliable is your telephone network? In the event of a communications failure do you have a contract with a third party maintenance company? Plan to be without landline phones for at least 5 hours.
- In a pandemic 25% - 30% of staff could easily 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 smaller business it is usually more difficult to cope with staff shortages. Would the business need to close down for the duration?
- Loss of electricity supply across a region could last 24 hours, although in areas exposed to significant weather effects 3 days might be a more realistic assumption. How long would nay on-site generator operate without re-supply?
- Assume that loss of water and or disruption to the sewerage services could last for 3 days.
- In a fuel crisis staff might struggle to get to work or you may not be able to make or receive deliveries. How long could you reasonably

expect to cope in this situation? The disruption to the transport network from a fuel crisis could easily last up to 10 days.

## 5. INSTRUCTIONS

Before completing the plan template it is essential to fully understand the processes and to collate sufficient background information to justify how the decisions and actions contained in the plan were arrived at.

- Firstly decide what are the essential processes or functions undertaken by the company. Where is the business most vulnerable? Deciding if a process is essential may depend on whether it has a direct impact on customers, finance, sales or production. A **Service Impact Analysis** will help to determine the priority processes. Those scoring highest will need to be included in the plan.
- Use a **Risk Assessment** form to identify the risks that have the potential to disrupt normal operations and where it might be possible to take preventative measures to significantly reduce their likelihood and/or impact.
- It will be necessary to fully understand how the business critical processes are currently structured to identify their strengths and weaknesses and to determine alternatives to cope with the loss of a building; staff shortages; the loss of IT or telecommunications; vital records; the failure of utilities such as power or water, or the loss of a key partner / supplier. This is a good opportunity to involve other members of staff in the discussion.

The completed plan must provide the information needed to maintain or restore the business following an incident but will also act as a useful reference document for dealing with day-to-day problems.

### 5.1 Service Impact Analysis

List each process / function / team or service identified in the left hand column. Complete the other columns according to the instructions below.

**Impact:** Consider:

- Does the process, when considered overall, have a direct impact on the business or customers? or
- Do they support a 'critical' service (that needs to be restored within 24hrs) elsewhere in the organisation?
- Is there a significant financial impact?
- Are the duties statutory?
- How necessary is the service in an emergency?

5 = vital	4 = high	3 = medium	2 = low	1 = non-vital
-----------	----------	------------	---------	---------------

**Restoration Priority:** Estimate the length of time you could operate before this process must be operating again:

5 = within 24hrs	4 = 3 days	3 = 7 days	2 = 28 days	1 = longer
------------------	------------	------------	-------------	------------

**Alternative delivery:** Could part or all of the work of that process be provided by alternative means, perhaps through another section or person, or by using temporary staff for a short period of time? Estimate how much of the service could be provided this way?

5 = none	4 = 25%	3 = 50%	2 = 75%	1 = 100%
----------	---------	---------	---------	----------

#### Analysis

Process / function	Impact	x	Priority	x	Alternative	=	Score
e.g. Sales Dept	4	x	3	x	3	=	36
		x		x		=	
		x		x		=	
		x		x		=	
		x		x		=	
		x		x		=	
		x		x		=	
		x		x		=	
		x		x		=	
		x		x		=	
		x		x		=	
		x		x		=	
		x		x		=	
		x		x		=	
		x		x		=	

## **5.2 Risk Assessment**

The risk assessment should identify the standard control measures plus any additional actions that could be taken to reduce the likelihood and the impact of the risk. Where appropriate these actions should be incorporated in normal day-to-day operational procedures

Examples of control measures include:

- Standard company policies and guidelines
- Additional staff training and procedure notes so that cover is available if key staff are absent.
- Security measures to prevent fire or theft.
- Reminding staff on good office practice such as not storing information on drives which are not automatically backed-up.
- Organising secondary users for e-mail and voicemail so they can be accessed in the event of absence, either planned or through illness.
- Identifying users of company laptops and mobile phone that could be reallocated in the event of a disruption.
- Ensuring that essential paper records are securely stored in fire proof cabinets or that electronically scanned copies are available.
- Checking that key partners or suppliers have business continuity plans. If a key supplier was unable to deliver materials your company may not be able to continue production.

Try to involve staff in identifying general control measures and further actions that can be taken to mitigate the risks. There may be other risks to consider such as a syndicate win on the lottery suddenly removing a whole team of people.

## ASSESSING THE RISKS

Use this table to provide an assessment of the current risks to the business and location. To reduce the risks make sure that all employees are familiar with any policies designed to improve health and safety at work. This table should be included in the back of the plan.

<b>Likelihood</b>	<b>Impact</b>
Low	Low
Medium	Medium
High	High

<b>Risk</b>	<b>Likelihood</b>	<b>Impact</b>	<b>General Control Measures</b>	<b>Possible Further Action</b>
<b>e.g. Fire completely destroying the premises</b>	<i>Low</i>	<i>High</i>	<i>Fire alarms and smoke detectors, Fire proof cabinets for vital records. Regular electrical safety checks. Small offices with fire doors reduce the chances of fire spreading. Fire and Evacuation plans tested and clearly displayed.</i>	<i>Enforce measures to reduce risks (e.g. clear desk policy, switch off equipment overnight. Staff trained to use fire extinguishers)</i>
<b>Fire completely destroying the premises</b>				
<b>Fire destroying part of the premises</b>				
<b>Theft of computer equipment</b>				
<b>Theft of office equipment</b>				

<b>Risk</b>	<b>Likelihood</b>	<b>Impact</b>	<b>General Control Measures</b>	<b>Possible Further Action</b>
<b>Loss of staff (Pandemic)</b>				
<b>Loss of key staff (Serious Incident/accident)</b>				
<b>Loss or corruption of IT systems</b>				
<b>Loss of telecommunications</b>				
<b>Loss of Electricity</b>				
<b>Loss of Water</b>				
<b>Loss of Gas</b>				
<b>Flooding</b>				
<b>Storm Damage</b>				
<b>Fuel Shortage</b>				

<b>Risk</b>	<b>Likelihood</b>	<b>Impact</b>	<b>General Control Measures</b>	<b>Possible Further Action</b>
<b>Vandalism</b>				
<b>Terrorist threat</b>				
<b>External factor preventing access to premises e.g. fire, police incident, traffic accident</b>				
<b>Industrial action</b>				
<b>Loss of a key partner or supplier</b>				

## **6. OUTLINE RECOVERY STRATEGIES**

This section of the guide will explain what background information needs to be collected and some of the options that could be considered. It will be worthwhile undertaking an 'end-to-end' analysis, from the start of the process through to completion to identify the strengths, weaknesses and possible breaking points.

### **6.1 Loss of Building / Accommodation**

If the building has been damaged, utilities have been severely disrupted or access has been prevented for some other reason then alternative accommodation may need to be found.

The first option will usually be a case of "budge-up" as people hot desk and share facilities. That may be fine for a few hours, even a few days, but if a large proportion of the office or factory space is out of commission and space is at a premium you will need to know in advance who needs to be accommodated first and where.

Options for alternative office space may include reciprocal arrangements with other local business or specialist disaster recovery sites.

Give careful consideration to minimum staffing levels. If a business is operating for any length of time with a low number of staff organise a rota of replacements to avoid fatigue or stress.

You may need to consider home-working or sending staff doing less business critical tasks home for a short period. This could even involve sending staff unaffected by the initial incident home to free up space and equipment for staff whose roles are more crucial.

Whatever the incident a process for communicating with staff must be in place. This may be a different process depending on whether the incident occurs in or out of office hours. A complete staff list with full contact details will be essential.

If existing accommodation is not accessible all office equipment and hard data in that building will probably also be unavailable. So you will need to consider how much of the existing office equipment would need to be replaced in order to maintain minimum services.

Replacement stationery may need to be ordered and telephones and post may need to be redirected.

Experience has shown that staff will need reassurance that there will be no adverse effect on their welfare or continued employment. If an accident has happened it is especially important that people are allowed to tell their spouse/partner or next of kin that they are safe.

At the earliest opportunity the staff should be briefed on the following points:

- What has happened
- What has been done
- What is planned
- How will the incident affect them

In the event of substantial damage to a building alternative accommodation that could be occupied for longer periods would be identified as part of the recovery plan. This could include the use of new buildings or Portakabins on the car park but these are longer-term solutions and are not likely to be an immediate option for restoring the business.

## **6.2 Loss of Staff**

Unless there was an event such as a fatal fire or explosion any large scale reduction in staffing, and the loss of key staff, is unlikely to occur without warning. A greater risk is a pandemic where up to 15 - 30% of the workforce could be absent due to sickness at any one time.

Document any steps that have or could be taken to reduce the impact of staff losses.

Plans need to consider measures to minimise the impact of the temporary or permanent loss of key staff. Staff training should ensure that specialist knowledge and skills are transferred so that in the absence of a key person somebody can fulfil their role.

Staff performing key tasks should be encouraged to write procedure notes so that less experienced staff would be able to perform these important duties in their absence.

Perhaps staff from a less business sensitive section could be used to supplement teams performing front line roles. Or perhaps agency staff or recently retired staff could be used. All of these options could be considered.

### **6.2.1 Recalling Staff**

If an incident results in staff either working from home or being sent home because there is insufficient space for them to work it is vital that there is a process in place for them to be called back to work. It may sound obvious but it has been forgotten before.

### **6.3 Loss of IT services**

Disruption to your IT network could be in isolation, due to a power failure or because of damage to the building. We all tend to take IT access for granted, but consider any actions that could be taken to cope with the absence of IT for a period of time.

Do you have maintenance contracts in place to provide a prompt response to any network failures?

To cope with loss of power laptops could be used to support important tasks. Compile a list of laptop users that could, if necessary, be reassigned. You will need to consider how batteries will be kept charged if power is down.

If the area relies on computerised information could it also be stored on a back-up disk or even as a paper copy?

It is worthwhile reminding staff not to store important data on any drive that is not backed up on a daily basis. All the information could otherwise be lost if that pc was damaged. Daily computer back-ups should always be stored at an alternative location.

Could manual processes be used as a short-term measure if IT access was unavailable? Is the temporary use of paper records a viable alternative until data can be transferred? Decide how records will be kept until they can be transferred onto the system.

### **6.4 Loss of telephone landline services**

Again disruption to telephone services could be in isolation or due to the loss of the building.

Do you have maintenance contracts in place to provide a prompt response to a telecommunications failure?

If the problem was isolated and only disrupting part of the network could calls be transferred to extensions that are unaffected?

List any actions that would be taken to cope without the telephone network. This could involve the use of personal mobile phones. The cost of any calls made with personal mobile phones would need to be reimbursed.

Consider compiling a list of company mobile phone users that could, if necessary, be reassigned. Make arrangements for phone chargers to be available.

### **6.5 Loss of hard data / paper records**

List any steps taken to preserve important data/records and how they can be retrieved.

The loss of vital data or records could be a serious setback to a business. Fireproof storage could help to protect records or electronic copies could be the solution.

If files need to be kept for any length of time scanning may be an option, although the cost may be prohibitive for records with a limited shelf life.

### **6.6 Loss of utilities**

The temporary loss of power is likely to be the most important consideration in terms of utilities. Staff need to be aware of the problems any disruption to utilities might cause and where possible take steps to reduce the potential impact.

Even where generators are in place the supply of power may not cover all the usual demands and electricity savings would need to be made.

Without power tasks usually performed on a computer will need to be handled manually unless there is access to sufficient laptops. Even if laptops are available they will need to be frequently recharged.

If the water supply was disrupted could you make arrangements to use nearby facilities and use bottled drinking water.

Failure in the gas supply could disrupt heating and cooking facilities in some buildings.

### **6.7 Disruption by industrial action**

You may not have any control over the industrial action. What would happen if a fuel crisis stopped you either making deliveries or receiving supplies? Or what impact would an extended postal strike have on your ability to bill customers.

### **6.8 Loss of a key partner or supplier**

Does your business rely on partners or suppliers?

- What would happen if a key partner went into administration, or the service was disrupted by industrial action?
- Could you source an alternative supplier at short notice?
- Could their loss disrupt the business or is there an alternative?
- Do key partners and suppliers have their own business continuity plans?

Also consider in what circumstances key partners or suppliers need to be told about any disruption to your business?

### **6.9 Severe Weather**

With more and more extreme weather events it makes sense to think about how you would cope if staff cannot get to work, either as a direct result of the weather, or if they need to look after children where schools are closed. What if supplies or deliveries are disrupted?

## **7. FINANCIAL ISSUES**

There may be additional costs involved with the recovery. This could include new equipment, special payments etc. The authorising of any additional expenditure in relation to the incident will need to be controlled. All expenditure should be monitored and recorded as it may be needed for insurance purposes.

## **8. MEDIA COMMUNICATIONS**

A major incident, such as a fire, may attract media or public interest and demand for information. The way that media and public information is managed will have a bearing on the public perception of the incident and possibly the reputation of the company.

## **9. RESPONDING TO AN INCIDENT**

### **9.1 Initial Response**

**During working hours:** The initial response to an incident that threatened the building or the safety of the staff would be to evacuate the building, or part of a building. Once the immediate danger has passed a decision will need to be made on whether it is feasible to return to work or whether the business continuity plan needs to be activated.

The initial response to any incident occurring **outside working hours** will depend on the type of incident, but staff may need to be contacted to advise them not to attend work. A list of staff home contact numbers will need to be available for this purpose.

### **9.2 Invoking the plan**

Staff need to be aware under what circumstances the plan would be invoked - by whom and why. The decision to implement the plan could be based on a predetermined percentage of disruption e.g. 15% of the building damaged, 20% of staff absent, or IT unavailable for more than 36 hours.

A localised incident might not class as an emergency but still represents a risk to the business and as such needs a prompt response and assessment. Some incidents will be dealt with as a day-to-day issue, but others due to their potential impact will need the business continuity plan to be invoked.

### **9.3 Action Checklists**

The plan includes two checklists **Form A – Immediate Actions Checklist & Form B – Response Actions Checklist** which suggest the actions that should be taken immediately an incident occurs and during the recovery phase. The lists are not prescriptive, exclusive or prioritised since any incident will require a dynamic assessment of issues and actions required. Include additional actions which are appropriate to your business needs.

## **10. COLLECTING THE BASIC INFORMATION**

It is important to have all the essential information readily to hand in the plan so it can be used immediately an incident occurs, effectively providing a shopping list for the restoration of the essential business processes.

The aim will be to recover services on a gradual basis by diverting the necessary equipment and resources to the most critical services.

- **Form C – Essential Services** is a list of the essential processes 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 minimum levels of accommodation and equipment needed to maintain operations.
- **Form E – Summary of Essential IT Systems & Records** summarises the basic software and systems data that need to be restored. This list should be used to prioritise work in the event of a major IT failure.
- **Form F – Staff Details** lists all staff, indicating those business critical staff that will be required if an incident occurs. If the information is already readily available in another format use that rather than compiling another list. The list should be reviewed regularly to make sure it is current.
- **Form G – Key Contacts** a list of those people that would need to be contacted in the event of an incident. This could be customers, key partners or suppliers. If the information is already readily available in another format use that rather than compiling another list. The list should be reviewed regularly to make sure it is current.
- **Form H – Plan Summary** provides a single sheet summary of the main recovery options of the plan.

## **11. TESTING AND REVIEWING THE PLAN**

Once the plan has been completed staff will need to be trained and tested on their roles and responsibilities. Someone will need to be made responsible for deciding how and when staff will receive training and making sure it happens.

Consider desktop exercises:

- To simulate a real crisis situation for the benefit of those taking part.
- To identify errors, omissions and areas of improvement in the plan.

- The plan should also be reviewed annually or when there are major alterations such as a change in location, organisation or responsibilities.
- The plan should identify who is responsible for maintaining and reviewing the plan.
- The plan revision should also include a progress report on actions taken to reduce the threat from individual risks e.g. enforcing a Clear Desk policy to reduce the spread of fire.

## **12. POPULATING THE TEMPLATES**

### **Form A – Immediate Actions Checklist**

The checklist in the skeleton plan is not prescriptive, exclusive or prioritised; any incident will require a dynamic assessment of issues and actions required. Include additional actions which are appropriate to your business needs.

### **Form B – Response Actions Checklist**

The checklist in the skeleton plan is not prescriptive, exclusive or prioritised; any incident will require a dynamic assessment of issues and actions required. Include additional actions which are appropriate to your business needs.

### **Form C – Essential Services**

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

*List the priority processes / functions that must be quickly restored. The service impact analysis will help to determine the priority. It may be just one process or it could be several.*

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

*List the additional processes / functions that must be restored within 2-7 days. These are over and above those that are required within 24 hours.*

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

*List the additional processes / functions that must be restored within 8 - 14 days. These are over and above those that are required within shorter periods.*

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

*Do any external partners rely upon your business in order to deliver their normal services?*

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

*Is there a dependency on external partners to provide transport, deliveries or other services without which your business might struggle to deliver its normal services?*

**Form D – Summary of Post Incident Resources & Equipment**

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

*In the event of a large scale incident all equipment could be in high demand and short supply. Only include the minimum requirements.*

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

**Form E – Summary of Essential IT Systems & Records**

*Prioritise the software or IT records that would need to be restored .*

*This information may be required by your IT section to help prioritise work in the event of a catastrophic IT failure.*

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

**Form F – Staff Details**

<b>NAME</b>	<b>POSITION/ROLE</b>	<b>KEY</b>	<b>ADDRESS</b>	<b>HOME</b>	<b>MOBILE</b>
<i>A Manager</i>	<i>Head of Section – would be responsible for organising the response in an emergency.</i>	<i>Yes</i>	<i>12 Swallow Road, Exeter, EX4 2DD</i>	<i>01392 222222</i>	<i>07929 121212</i>
<i>A Secretary</i>	<i>Secretary – needed to provide secretarial support to A Manager</i>	<i>Yes</i>	<i>10 Rook Close, Exeter, EX5 3FF</i>	<i>01392 333333</i>	<i>07813 212121</i>
<i>A Clerk</i>	<i>Clerical Officer</i>	<i>No</i>	<i>53 Kestrel Avenue, Exeter EX2 5HH</i>	<i>01392 444444</i>	<i>07801 313131</i>

If this information is held in another format do not bother to replicate it. Simply state who has access to the alternative list or where it is stored for easy access. Remember to keep a paper copy in case your IT system is not accessible.

Frequency of updating a staff list depends on the size and turnover of staff.

**Form G – Key Contacts**

**(Other internal staff contacts, external contacts).**

<b>NAME</b>	<b>POSITION/ROLE</b>	<b>E-MAIL ADDRESS &amp; OR BUSINESS PHONE</b>	<b>HOME</b>	<b>MOBILE</b>
<i>A Major supplier</i>	<i>Delivery Manager</i>	<i>Major.supplier@bigco.co.uk 01392 777777</i>	<i>01392 222222</i>	<i>07929 121212</i>
<i>A Press</i>	<i>Reporter on local paper</i>	<i>Apress@myco.co.uk</i>	<i>01392 279999</i>	<i>07929 454545</i>

If this information is held in another format do not bother to replicate it. Simply state who has access to the alternative list or where it is stored for easy access. Remember to keep a paper copy in case your IT system is not accessible.

The frequency for updating a key contact list depends on the numbers involved and the turnover of suppliers / customers etc.

**Form H – Summary of the Business Continuity Options**

<b>Identified Risk</b>	<b>Recovery Option</b>	<b>Evaluation Criteria</b>	<b>Possible Further Action</b>
<b>Loss of accommodation</b>	<i>State the preferred locations for alternative accommodation</i>	<i>Justify how this decision was made.</i>	<i>Is there an alternative if the first choice options were unavailable?</i>
<b>Loss of Staff</b>	<i>What are the options if there were insufficient staff to fulfil all normal services?</i>	<i>Justify how this decision was made.</i>	<i>Could other staff be used to cover the absent staff? What steps have been taken in terms of process notes and training?</i>
<b>Loss of IT / Data</b>	<i>How would the processes work without IT? Manual process, laptops etc.</i>	<i>Justify how this decision was made.</i>	<i>Is there anything else that could be considered?</i>
<b>Loss of Telecommunications</b>	<i>How would the process work without landline telephones? Divert to mobile?</i>	<i>Justify how this decision was made.</i>	<i>Would phone chargers be available? Is a list of phone users readily available?</i>
<b>Loss of Hard Data / Paper Records</b>	<i>How would important records be recovered? Are they available electronically?</i>	<i>Justify how this decision was made.</i>	<i>Is the existing storage fireproof? Could copies be held off site? Is scanning an option?</i>
<b>Loss of Mains Services</b>	<i>Actions may be covered by a site plan at larger establishment. But how would you cope without power, water or gas for any period of time?</i>	<i>Justify how this decision was made.</i>	<i>Is there a generator to provide power? Could a nearby business be persuaded to allow temporary access to their facilities?</i>
<b>Loss of a Key Partner / Supplier</b>	<i>What is the process if a key partner is unable to deliver a service?</i>	<i>Justify how this decision was made.</i>	<i>Are there any other alternatives?</i>

Identified Risk	Recovery Option	Evaluation Criteria	Possible Further Action
<b>Disruption due to industrial action</b>	<i>Are there alternatives if industrial action causes disruption?</i>	<i>Justify how this decision was made.</i>	<i>Are there any other alternatives?</i>
<b>Loss or disruption to the transport network</b>	<i>Are there alternatives methods of delivery?</i>	<i>Justify how this decision was made.</i>	<i>Are there any other alternatives?</i>
<b>Severe Weather</b>	<i>Are there alternatives methods of working or delivering services?</i>	<i>Justify how this decision was made.</i>	<i>Are there any other alternatives?</i>

### 13. ANNEX

#### Company Mobile phone users

<i>List all users of company mobiles that could be utilised if landlines were unavailable.</i>	

#### Laptop users

<i>List all users of laptops that could be reassigned if desktop pcs were unusable</i>	

#### Staff able to work from home

<i>List staff who can access systems from home</i>	

#### Emergency Operations Log

<b>Team / Section:</b>		<b>Date:</b>	<b>Sheet ..... of .....</b>
<b>Time</b>	<b>Event</b>	<b>Action</b>	
	<i>Use this to record actions taken if an emergency occurs</i>		

*Could also include a copy of fire / evacuation processes in the back of the business continuity plan so they are readily to hand in the event of an incident occurring.*

**END**