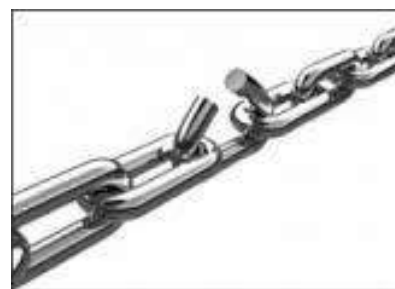




Building Business Resilience

A Business Continuity Guide for Local Businesses
and Voluntary Organisations

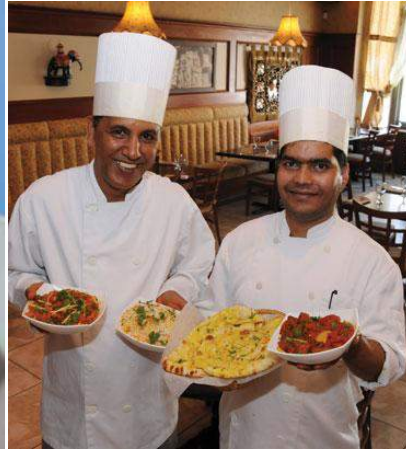


FOREWORD

The Civil Contingencies Act 2004 introduced a responsibility on all local authorities to raise the awareness to their local business community of the importance of Business Continuity Management (BCM).

Located in the heart of Essex, Brentwood is a pleasant, busy town, conveniently situated for London and the surrounding countryside and coast. Distributed widely around both the urban and rural areas of the Borough, Brentwood has seven industrial and commercial estates and parks. In addition, there are concentrations of commercial activity in Brentwood Town Centre, Shenfield, Ingatestone and Warley. There are approximately 5,000 businesses in Brentwood employing nearly 40,000 people.

Brentwood Borough Council prepared this booklet to provide general information about BCM. It was distributed to registered businesses in the district during 2015 and is available on the Council's website at www.brentwood.gov.uk



Contents

Would your business survive a crisis?	1
What type of incidents should I plan for?	4
5 Step Guide	6
Frequently Asked Questions	9
Ten Top Tips	10
10 minute checklist	11
Business Continuity Plan	18
Initial Recovery Log	32
Useful Contacts and Links	33



Would your business survive a crisis?

FACT: Every year 1 in 5 businesses face a major disruption to their service

FACT: 1 in 10 of these will cease trading

If your premises were to suffer a fire how would you maintain your essential business functions?

How would you ensure your business survives?

A crisis that threatens the survival of your business could happen at anytime.

The most common threats to your premises, flood, fire, power failure, break-ins/vandalism are independent of size, and are the same whether you run a large business employing many staff or a family corner shop. The effects are potentially devastating.

Planning for the continuity of your business in an emergency is essential.

Start now – you never know what tomorrow can bring.





What would happen if your business was involved in a major incident?

What is it?

Everyone hopes that they will not be affected by a major incident or disaster. If we are affected, we hope that “someone, somewhere” will know what to do. We know that any serious incident will be dealt with initially by the emergency services but do we know what will happen next?

- How will we be kept informed?
- How will we get back to business?

This is where Business Continuity Planning (BCP) comes in. Any number of events can bring businesses grinding to a halt and the purpose of Business Continuity Planning is to ensure that we can respond sensibly, as a company and as individuals.

Put simply, business continuity is about anticipating the crises that could affect a firm and planning for them.

A Business Continuity Plan will identify all the requirements, which are essential to keeping your business running, and will include processes to keep disruption to a minimum. It is about ensuring that we can manage a crisis effectively.

The information contained in this booklet aims to assist you in producing a Business Continuity Plan for your own business and to provide sources of further information for your future use.

The Law

The Civil Contingencies Act 2004 requires organisations designated as Category 1 responders (emergency services, A&E hospitals, Primary Care Trusts, local authorities, Health Protection Agency, Maritime & Coastguard Agency, Environment Agency) to maintain plans to respond to emergencies. It also requires them to make provision for ensuring that their ordinary functions can be continued.

The Act also requires local authorities to provide advice and assistance to businesses and voluntary organisations in relation to business continuity management. This duty is an integral part of the Act's contribution to building the UK's resilience to disruptive challenges.

What type of incidents should I plan for?

Depending on your business' specific circumstances, there are many possible events that might affect your ability to operate.

Incidents that could affect your business:

- **Severe weather** – for example, flooding caused by heavy rain, or wind damage following a storm. If your business is in a remote location you may be more susceptible to this type of disruption.
- **Theft or vandalism** – theft of computer equipment, for example, could be very detrimental. Similarly, vandalism of machinery or vehicles could not only be costly but also pose health and safety issues.
- **Fire** – few other situations have such potential to physically destroy a business.
- **Loss of utility** - loss of power or water could have serious consequences. What would you do if you suffered a loss of heat and light or couldn't use IT or telecoms systems or operate other key machinery or equipment.

-
- **IT system failure** – computer viruses, attacks by hackers or system failures could affect employees' ability to work effectively.
-

- **Disruption to fuel supplies** – would you be able to operate company vehicles in the event of a fuel crisis, would your staff still be able to get to their workplace, or would your suppliers be able to deliver goods to you?
-

- **Restricted access to premises** – how would your business function if you could not access your workplace – for example, due to a gas leak?
-

- **Illness of key staff** – if any of your staff are central to the running of your business, consider how you would cope if they were incapacitated by illness.
-

- **Outbreak of disease or infection** – depending on your type of business an outbreak of an infectious disease among your staff, for example a flu outbreak, in your premises or amongst livestock could seriously deplete your workforce or present serious health and safety risks.
-

- **Malicious attack** – although this is less likely for small businesses it may be worth considering the risk of malicious incident (e.g. animal rights groups) depending on the nature of your business. If you're based in a large city you may suffer the effects of an attack on a neighbouring or shared building.
-

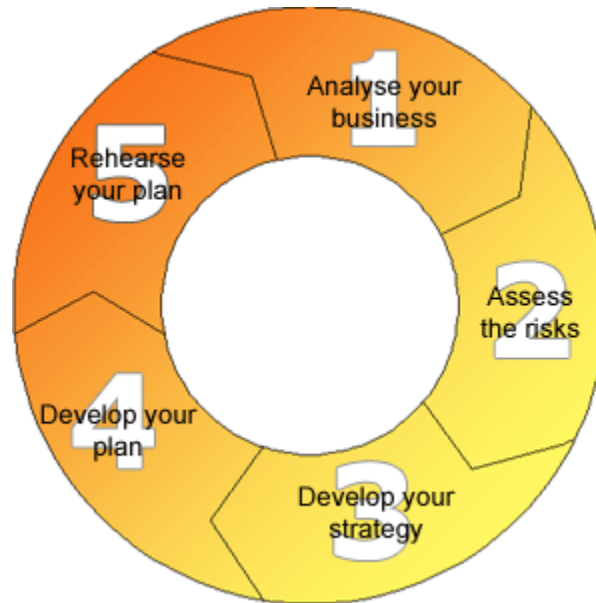
- **Disasters affecting suppliers** – how would you source alternative suppliers?
-

- **Disasters affecting customers** – will insurance or customer guarantees offset a client's liability to take your goods or services?
-

Although you may feel that some of these situations would not affect your business, it's sensible to give them consideration.

5 Step Guide to Business Continuity Planning

You will find that it is quick, easy and inexpensive to create a business continuity plan. This is a basic five-step guide to get you started on business continuity planning.



Step 1: Analyse your business

Step 2: Assess the risks

Step 3: Develop your strategy

Step 4: Develop your plan

Step 5: Rehearse your plan

1. Understand your business and what makes it tick

- What is the purpose of your business?
- How is that achieved?
- What are your products/services?
- Who is involved (internal and external)?
- What deadlines do you work to?

2. Assess the risks to your business

What could affect your business (internally and external)?

- Power cuts
- Staff illness/lottery win
- Fire
- Flood/water leak
- Theft/break-in
- Unable to gain access

3. Develop your strategy to deal with those risks

A strategy will protect your business – it will identify:

- What needs to be done
- How 'actions' need to be done
- Who needs to perform these 'actions'
- Why 'actions' are needed
- Where 'actions' should be performed i.e. on site or at a different location

4. Develop your plan

The plan can be as simple as you want – the simpler it is the more flexible it will be.

i.e. if there has been a fire – what do you need to do first, do you need to connect telephones first to contact customers, does this need to be done at an alternative site, do all of your staff need to relocate to this alternative site – or can some of them work from home etc?

5. Test and update your plan

It is essential to update your plan on a regular basis and each time something changes, for example, changes in supplier contact details. Remember to inform your insurance company things have changed.

It is also essential that the plan is tested. Involve all of your staff and familiarise them with their roles and what to expect.

Frequently asked questions

What is a business continuity plan?

A business continuity plan should be a set of instructions of what to do and what not to do at the time of a crisis. It is about thinking ahead and planning for any crisis which could affect your business. The plan should set out clear roles and responsibilities and list a series of actions which allow key business activities to continue in the most difficult circumstances.

How does business continuity planning differ from a disaster recovery plan?

Disaster recovery plans traditionally focus on the IT recovery of the business. A business continuity plan addresses all the essential requirements to keep the business running. In addition it should include processes to keep disruption to customers and employees to a minimum.

How long will it take to create a business continuity plan?

It should not take long to create your first plan, but obviously this will depend upon the complexity of your business. The smaller the size of your business generally the less time it is likely to take. Later in this guide there is a template for you to refer to when drafting your own continuity plan.

What will it cost to create a business continuity plan?

The cost will be relatively little and at the end of the exercise you will have a plan to protect your business. The benefits of having a working continuity plan will outweigh any small expenditure. The price of not planning could be a lot higher than many companies anticipate.

Isn't my business too small to have a business continuity plan?

No, even a sole trader is advised to have systems in place to be able to continue work in case of theft, fire, flood, IT and utility failures, etc. Any incident, no matter how small, is capable of impacting your business and profitability. The size of any plan will depend on the risks facing each business – it will be as large or small as needed.

Ten top tips for Business Continuity

- 1** Plan for the effects of an incident, not the cause. At the time of a crisis what happens may well be more important than what caused it.
- 2** Remember that prevention is better than cure.
- 3** Test systems, exercise plans and rehearse the people involved on a regular basis. Maintain the plans – keep them up to date, build in a regular review of your plan.
- 4** Back up data regularly and store copies off site in a secure place. Practice restoring the data in an IT system outside your own to ensure that it works.
- 5** Ensure that important paper documents, such as contracts and employee information are protected. Make copies and use fire resistant and waterproof storage.
- 6** Keep a list of contact details for your staff, customers and suppliers off-site so that you can contact them if you do not have access to your usual premises. Review regularly.
- 7** Be clear about what your insurances cover and what they don't. Keep copies of the relevant policies off-site so that you know immediately what to do in the event of an accident.
- 8** Have an emergency pack which will include your business recovery plan, key telephone numbers, as well as a first aid kit, torch, megaphone, spare keys, cash, credit card, stationery, etc.
- 9** Make arrangements for a temporary base – you may not be able to operate out of your existing premises for weeks or even months. Remember, any temporary accommodation still has to comply with health and safety rules.
- 10** Make an inventory of equipment, materials, products and any other assets to give you an overview of the business. This will make it easier to work out losses and identify gaps in core resources after an incident.

The 10 minute checklist

This is a quick assessment for business continuity planning. The assessment has been split into sections for ease of reference. Ideally you should have all of these criteria fulfilled.

	YES	NO	DON'T KNOW
Do you have a Business Continuity Plan (BCP)?			
If yes, have you tested and reviewed your plan within the last 12 months?			
Do you have a policy for when to activate your plan?			
Do you regularly train staff and test your plan?			
Has the idea of Business Continuity planning been approved by the board/owner/partners?			
Is there someone in your organisation who will have responsibility for looking after a BCP?			
Is the plan documented clearly and easily accessible?			
General Assessment			
Have you made a list of all key contacts' telephone numbers?			
Have you got a list of all employees' telephone numbers?			
Do you have vital computer information stored on back up disks (or paper copies) held off premises?			

	YES	NO	DON'T KNOW
Have you familiarised yourself and your staff with the location of the mains switches and valves (i.e. for electricity, gas and water)?			
Have you checked that all plumbing is in working order?			
Do you check that the heating and air conditioning is working on a regular basis?			
Have you prepared an emergency pack?			
If you have prepared a pack have you included the following essential items:			
Business recovery plan			
List of employees with contact details?			
Details of IT providers			
Contact details for clients and suppliers			
Building site plan			
Spare keys			
Computer back up tapes/discs			
First aid kit			
Stationery			

	YES	NO	DON'T KNOW
If you haven't already you might also want to include these useful items:			
Torch			
Megaphone			
Tape to cordon off areas			
Message pads and flip charts			
Coloured pens and pencils			
Mobile telephones (with credit)			
Dust and toxic fume masks			
Disposable cameras			
Petty cash and/or credit card (staff may need emergency funds)			
What do you do on a day-to-day basis?			
Do you carry out end of day inspections? i.e. to check everybody has left			
Do you make sure that all appliances are switched off?			
Do you check that all doors and windows are locked?			
Do you make sure that you have a clear desk policy? (All paperwork filed or stored away)			

	YES	NO	DON'T KNOW
Building Facilities:			
Do you have evacuation procedures for your building and are staff trained in them?			
Are the fire exits clearly marked?			
Do you regularly practice fire drills?			
Do you have primary and secondary evacuation points?			
Do you have a floor plan to your building?			
Does your building(s) require 24-hour 7 days a week access?			
Do you have generator back-up systems in place and do you know how to activate them?			
Do you have an alternative building to use in an emergency?			
Personnel			
Do you have up to date and regularly reviewed job descriptions and organisational chart for your company? (Include temporary and contract workers)			
Do you have staff personal information on file i.e. communication with next of kin? (Include temporary and contract workers).			
Do you and your staff know what to do in an incident?			

	YES	NO	DON'T KNOW
Do you know where to go for advice/information?			
Do your staff know who is in charge in the time of a crisis?			
Have your staff been given specific roles to do in the event of a crisis?			
Have you thought about dealing with people issues – relocation arrangements, etc?			
Transport home – staff may have to leave without coats, bags, cash, keys (home/car)			
Do you have members of staff with first aid or medical training?			
Security:			
Is there a security system installed?			
Do you have a security policy?			
Do you give any advice or training on security?			
Do you check references fully?			
Are contractors checked fully (i.e. company as well as individual)?			
Do you regularly check the integrity of external fences and doors?			

	YES	NO	DON'T KNOW
Company Equipment			
Do you have someone in your company accountable for the assets/stock of your company?			
Do you have controls over the movements of your company equipment/stock?			
Have you completed a recent inventory of your company equipment/stock?			
IT			
Are your IT systems critical to the running of your business? (phone/credit card system/cash tills)			
Do you have a tested IT disaster recovery plan?			
Is your computer anti-virus software up to date?			
Are computer errors and logs adequately monitored?			
Are documented IT security policies and procedures in place?			
Are all computer users fully aware of e-mail and internet usage policies?			
Do you know how many platforms/servers/applications or operating systems support critical business functions?			
Is your company system part of a larger network?			
Do you know how long it would take to recover IT functions?			

	YES	NO	DON'T KNOW
Suppliers:			
Do your key suppliers have a business continuity plan? (you may have to rely on them)			
Customers			
Do you have the correct contact details for all your customers?			
Do you have any key customers who you will need to be in constant contact with during a crisis?			
Would it affect your business if one of your key customers went out of business?			
Do your customers require that you have a BCP?			
Location:			
Have you thought about the types of risk that might occur due to the actions/operations of other businesses near to you? i.e. sewage works / risk of pollution / smoke damage / water leak from business above			
Have you thought about the types of risk associated with environment? E.g. water/flooding, climate change, etc.			
Insurance:			
Do you have sufficient insurance to pay for disruption to business, cost of repairs, hiring accommodation and equipment?			
Do you have your insurance company's details in order to contact them immediately at the time of the incident?			

Business Continuity Plan for:

(insert your company name here)

Our Statement of Business Continuity is:

- To ensure all employees are competent to do their tasks, and to give them adequate training
- To review and revise this plan on a regular basis
- To provide a general plan on what to do in an emergency situation
- To provide details of emergency contacts – staff/suppliers/customers
- To ensure that the business continues

Signed

Position in company

Review date of plan

Responsibilities

Overall responsibility in any incident is:

Day to day responsibility for this is (if different to above)

(Name) is responsible for checking on a regular basis:-

Fire alarms

Security alarms

IT systems security

Health & safety

Power supplies

Flooding

Person responsible for compiling/maintaining:-

Insurance cover is up to date

Staff contact no's
(inc. next of kin details)

Customer contact numbers

Supplier contact numbers

Power/generators

UPS/IT systems

Description of your premises

Location of the emergency exits



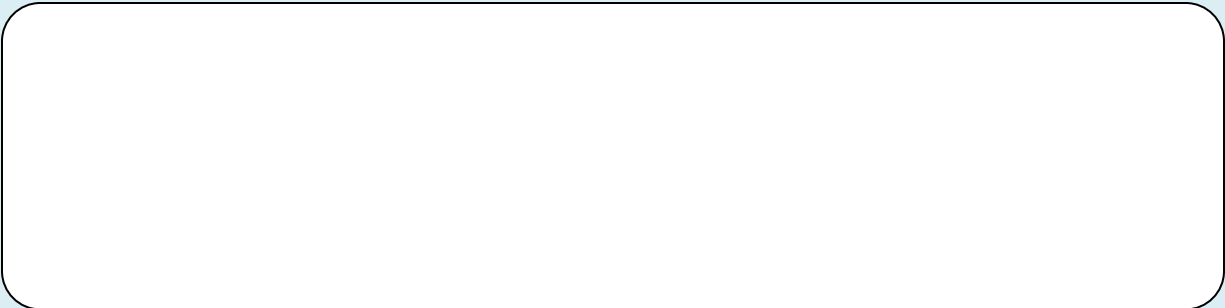
A primary meeting point in case of evacuation



Attach map if possible

In case of fire this should be at least 50m away, or for a bomb scare 800m

A fall-back option if you have to evacuate in a different direction



Attach map if possible

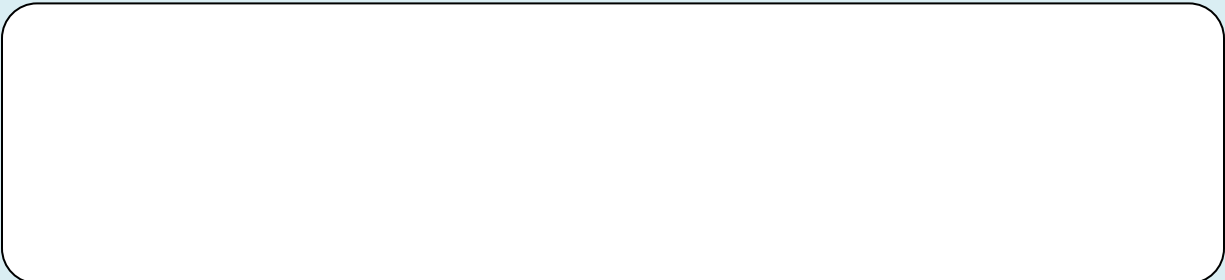
Details of what the premises contain



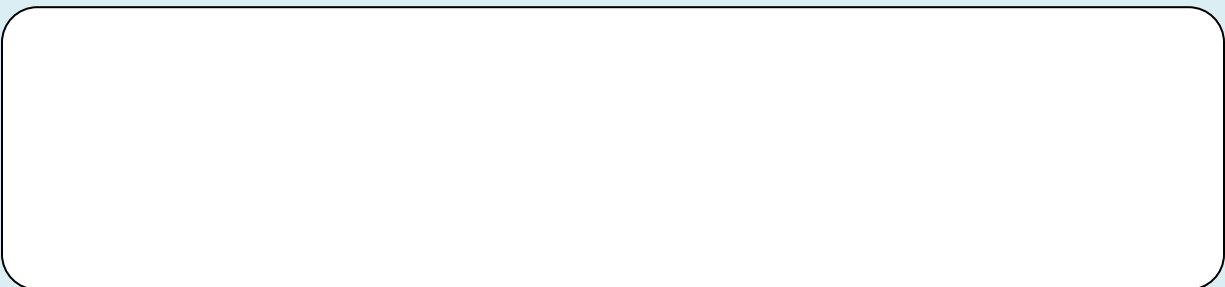
Information that is important and specific to your premises e.g. storage facilities



Essential and useful contact details



Essential and useful items



Software and hardware inventory lists, plans and contact details that you should have on and off-site:

Structure of the “crisis team” for Business Continuity

Owner of business	<input type="text"/>
Manager	<input type="text"/>
Supervisor	<input type="text"/>
Floor Manager	<input type="text"/>
Media/Public Relations	<input type="text"/>
Administrative Support	<input type="text"/>

Everyone in your business should know when emergency plans should be implemented and who has the authority to implement it. The plans should specify everyone who is responsible for initiating their implementation.

Allocate a list of suitable locations where your Business Continuity team should meet if an incident occurs. This should consist of a room on-site or a place in a public building e.g. local hall, someone’s house or a meeting room at your alternative fall-back site.

If an incident occurs, meet with everyone from the BC team as soon as you can.

Critical Systems



List the systems which are critical to your business e.g. order taking, dispatching goods – how and where will these operations be continued following a disaster? In addition make notes on your recovery time objectives so you can prioritise your recovery process appropriately and the activities you will need to undertake after the first hour of the incident.

Work Area Recovery

List areas of work in priority order



Can staff work from home temporarily? – list names



Have you made arrangements to use another company's facilities, if so, give details?

There are business continuity suppliers who will arrange agreements for you to use other premises or get a temporary structure erected for your use. This can result in you having alternative accommodation within 4 hours but is a relatively expensive option.

Recovery site location

List the alternative location(s) that your firm will use if your main premises are unavailable. Include a floor plan, map and telephone number of recovery site location(s).

Relocation of staff

Will your staff need transport or accommodation if you are operating from different premises? It would be useful to list the means of transport your employees could use to reach this facility.

Facilities available if an alternative site is proposed

Disabled access, parking, catering facilities, telecommunication links, security, arrangements for mail, etc.

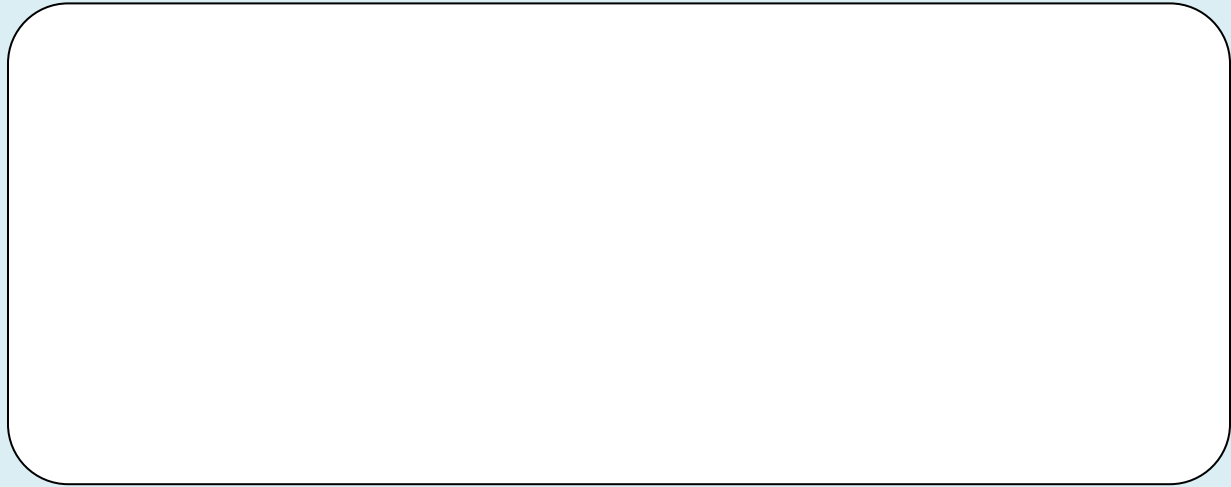
Technology Recovery

Most businesses have complex IT, telecommunications and utilities structures in place. It is imperative to keep an inventory list so that you can replace equipment immediately if needed. It is worth checking in advance if your insurance covers the replacement of damaged items immediately or whether you need the insurance company's consent.

Inventory list of software and hardware

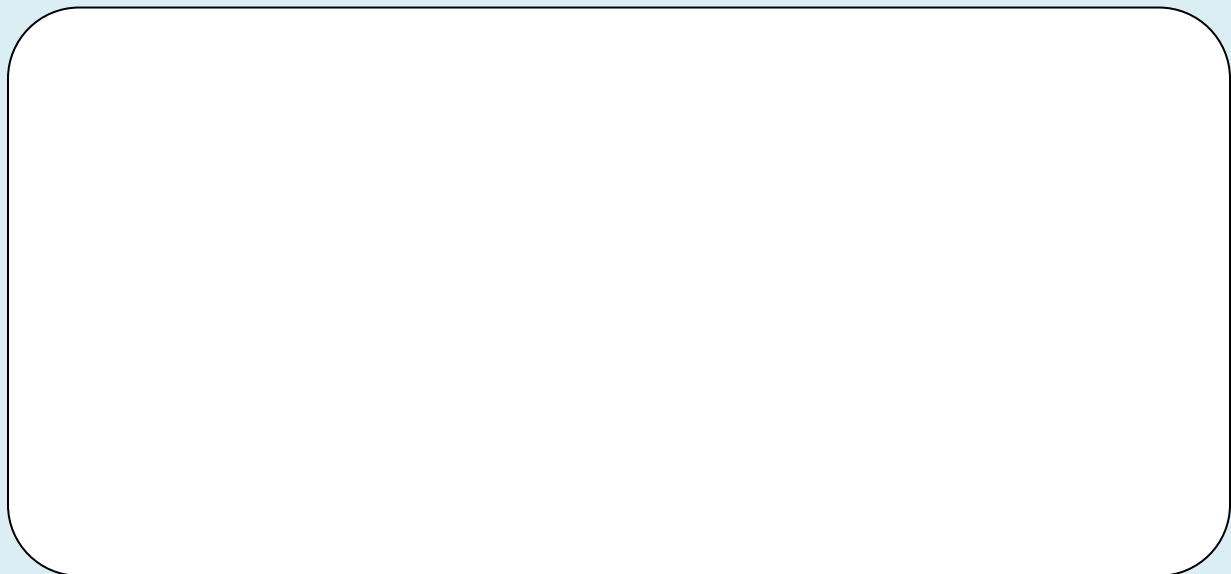
Number of workstations and software applications required at each station (minimum number).

Backed up data



Where is this held and by whom? Who will be responsible for re-installing this on your equipment? Describe how you will recover data in the event of an incident.

General office equipment and stationery required station (minimum number)



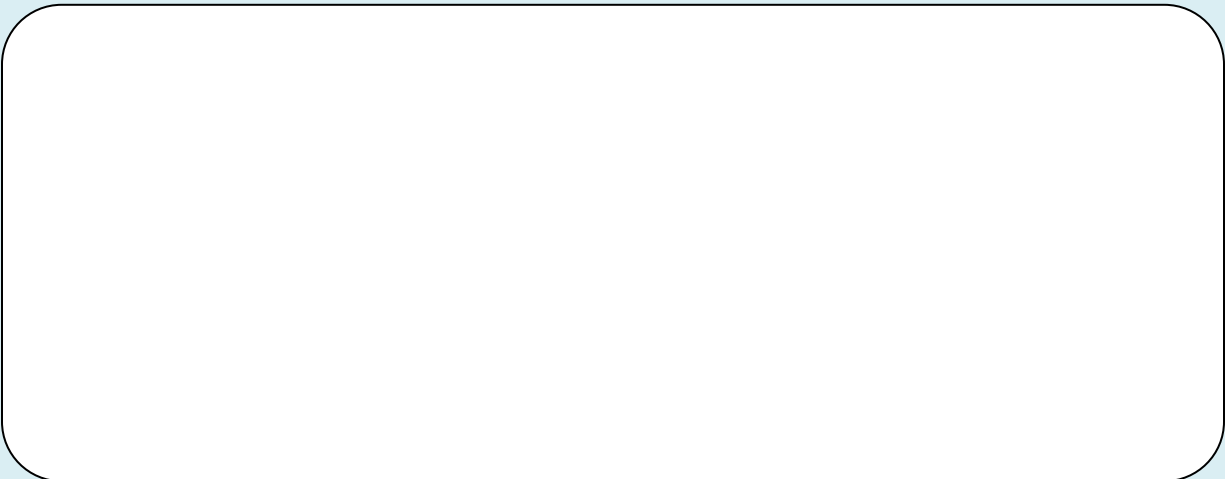
Telecommunications

Contact list



Make a list of all access numbers and keep them safely with all your important documents on and off-site. Check whether you have the capability to access your telephone system remotely from another site. Make sure all relevant programming is undertaken as soon as possible.

Alternative Communications



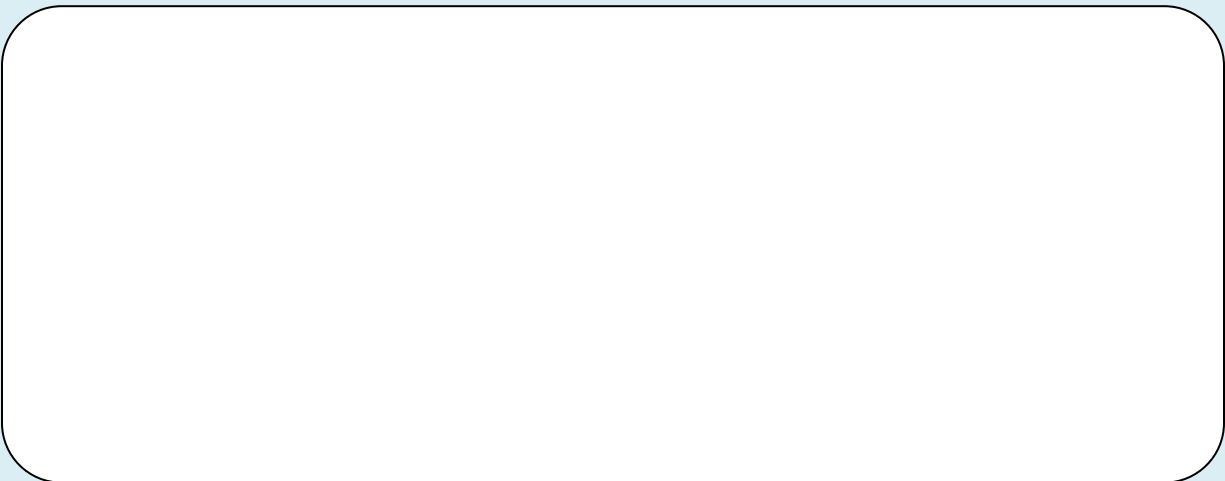
Describe the alternative means of communications your business will use to communicate with customers and employees in the event of an emergency.

Utilities



In the case of a utilities failure, make sure you have a list of your utilities providers, their contact details and your account numbers. You may want to acquire an 'old style' telephone handset which you can plug directly into a telephone socket. This has its own power source via the line and will not be affected by a power cut.

Public Relations



The PR process can greatly affect the way your company is perceived and in many instances can make or break a company's reputation. Remember that PR will influence how your customers (or potential customers), suppliers and all other stakeholders will react to the incident.

Details of Company's spokesperson(s)

Ensure that your staff know who the spokesperson will be. Nominate more than one staff member in case anyone is not available and ensure that the nominated members of staff have some training in media handling.

You may wish to have a “holding statement” prepared so you can give early information to the press which can be followed up with more detailed information at a later time.

Local press contact details

You may wish to place advertisements in the local press or supply press releases on your current situation and intended actions.

NB. If you cannot keep all your staff on-site during an incident you will need to consider ways of keeping them well informed about progress too.

Testing

It is important to ensure that relevant people in your company – and in other organisations if appropriate – are confident and competent concerning the plan. You should consider developing and running a training programme for those directly involved in the execution of the Business Continuity Plan. If you test the plan before you have trained the staff it will be impossible to tell if it is the plan that has failed or the lack of knowledge which has stopped it being effective.

Testing your Plan

Date(s) of Test carried out:

Once you have developed your plan it should be subjected to rigorous testing. You will never know if you have omitted something if you don't test your plan. It is vital to test the plan with all the appointed business continuity team members to ensure they are fully aware of their responsibilities.

Give your staff an opportunity to ask questions and clarify issues as they may highlight areas which need to be considered or amended.

Review

It is important to review your plan regularly and keep it up to date. Particular attention may need to be paid to:

- Staff changes
- Changes in the organisation's functions or services
- Changes to the organizational structure
- Details of suppliers or contractors
- Changes to risk assessments
- Business objectives/processes

It is important to ensure all information in this plan is as clear and simple as possible – it may be that someone else has to follow the plan – you may not be on site.

Initial Recovery Log

Maintaining this log will provide a record of all events, actions and decisions taken. It should include the names of those instructed, timings and action taken (it will also help in insurance matters if necessary).

Date	Time	Information / decisions / instructions / actions	Initials

Further Advice / Information

Brentwood Borough Council cannot write or test business continuity plans. However we are happy to provide advice and guidance to businesses in the District. Further information about business continuity can also be found at the following websites.

Brentwood Borough Council

<http://www.brentwood.gov.uk>

Essex Resilience Forum

www.essexprepared.co.uk/prepare-your-business

Business Continuity Institute

www.thebci.org

Small Business Service

www.smallbusiness.co.uk

GOV.UK – Emergency Planning

www.gov.uk/government/publications/business-resilience-planning-assumptions

MI5 – security advice for business

www.mi5.gov.uk