Trinity Harper
Cleaning Ltd

01223 782505
www.trinityharpercleaning.co.uk

Business Continuity Policy

A) FIRE PROCEDURES

Fire procedures are displayed in prominent positions, on notice boards, around the workplace. They include the identity of appointed Fire Marshals, emergency exits, the location of muster points and other procedural details. All employees must ensure that they are familiar with the emergency procedures in order to minimise the risks to life in the event of an emergency situation caused by fire.

You should familiarise yourself with all emergency escape routes, the location and types of firefighting equipment available and how to use it.

There are appointed Fire Marshals in each area of the building; it is their responsibility to instigate and coordinate the effective evacuation of the area in the event of an emergency requiring immediate evacuation. If the fire alarm sounds, you must follow their instructions. Once the building is clear a register will be taken to ensure all employees are accounted for.

It is important to practice fire procedures to ensure that they remain effective and practice evacuations will take place periodically. These drills should be treated seriously and as real fire emergencies by all employees.

If you have issues which will affect your ability to evacuate the building you should inform the Fire Warden who will arrange for assistance.

If an employee discovers a fire, they should:

- raise the alarm, operate the nearest call point
- inform the responsible person of the location of the fire
- only fight a fire if you are trained or are competent to do so
- do not put yourself or others at risk by stopping to fight a fire.

If an employee hears the activation of the fire alarm, they should:

- do as instructed by Fire Marshals
- evacuate in a timely manner without delaying to retrieve personal items
- do not hinder other people's evacuation
- do not use lifts
- remain calm, walk quickly and do not run

- remain at your muster point until instructed otherwise
- do not re-enter the building until instructed by a Fire Marshal.

B) BOMB SCARE PROCEDURES

Upon discovery of a suspicious object, package or threat of an explosive device you must be ready to assess the risks to yourself and others in the area. Following assessment of the situation you must decide on appropriate actions and act accordingly.

Telephone Warnings
If an employee is made aware of a bomb scare by telephone, they should:

- ensure they allow the caller to deliver the full message, stay calm, do not interrupt them before engaging in conversation
- keep the caller on the phone for as long as possible whilst attracting the attention of a colleague
- inform the colleague in a discreet manner, indicating them to inform the responsible person
- take note of anything about the caller that may be useful to the authorities including; accents, sex, any background noises and the type of language used
- the responsible person will instigate appropriate action with guidance from the emergency services.

Suspicious objects/packages
If an employee is the recipient of a suspicious object or a package, they should:

- evacuate people in the immediate vicinity of the device/package and ensure that no one tampers with it
- inform the responsible person of the issue immediately.

Evacuation procedure
If an evacuation is deemed to be appropriate, Fire Marshals will instigate the evacuation procedure. It is important that you listen to their instruction as the evacuation plan may change depending on the nature of the threat.

Make sure that their instructions are followed as this evacuation may have been instigated by the emergency services.

C) INFECTIOUS DISEASE PROCEDURES

Where it is recognised by the World Health Organisation or the Government that an infectious disease creates a public health emergency, the Company will assess the risk posed to its workforce by the disease.

At all times, Government advice will be followed on managing our employees in relation to infection control, overseas travel, isolation periods and other relevant matters.

With regard to the severity of the risk, we may decide to:

- stagger start and finish times so that fewer people are together at once
- cancel non-essential overseas travel to affected areas across the world
- cancel non-essential training sessions
- deal with clients/customers by phone, email or video call
- if face to face meetings must take place, ensure that facilities are suitable to minimise the spread of infection
- deploy greater levels of flexibility including permitting employees who are usually office based to work from home.

Employees have a role to play in ensuring that the risk of infection is kept at an absolute minimum, and must themselves stick to Government guidance in relation to overseas travel etc.

D) BUSINESS CONTINUITY MANAGEMENT PLAN (BCMP)

Our Business Continuity Management Plan outlines how we plan to continue business in a variety of circumstances which are applicable to the business, regardless of how farfetched scenarios may seem.

The steps below form a structured approach to ensure that in the event that key business assets are lost continuity is maintained with minimal effects on the business.

Like emergency evacuations, we will test the plans to ensure their suitability and effectiveness.

Step one - introduction
In brief, the BCMP outlines the organisation, its interested parties and how long full implementation of the plans should take to ensure loss of service or production is minimal. The introduction also outlines the aims and objectives of the plan.

Step two - roles and responsibilities
This step sets out the contact details of those who are responsible for:

- development of the plans
- operation and testing of the plans and
- those with the authority of activating and escalating the plan.

Additionally, the process for invoking the plan is also outlined in brief. Those who may be required to put the plan in motion should be aware of this.

Step three - BCMP team
The team is made up of the key staff who will be mobilised to invoke the plans after approval from those with the authority for activation. This section contains:

- details of the team, their allocated tasks and how to contact these.
- a pre-defined location to run and coordinate business activities from
- location and contents of an emergency kit containing what is required as a minimum to ensure that business activities can be undertaken.

Step four - other contacts
The details of other key contacts who have an impact on the effectiveness of the Business Continuity Management Plan are included, examples of this could be suppliers, emergency services etc.

Step five - risk register
A register of tasks categorised by the level of impact they have on the organisation's continuity of business and safety, health and welfare will be maintained. Management will implement controls suitable to the situation and ensure that they are communicated to employees.

Step six - other information
Any other information that might be applicable in any given circumstance will be detailed, this may include utilities suppliers, councillors, provisions for communicating with employees, the media and what transport, if any will be utilised.

Step seven - action plans
Recovery plan
The recovery plan ensures that critical business activities, as identified in the risk register, can be resumed following, or during, serious damage/incident.

This may involve ensuring that employees will conduct normal working tasks from home. Alternatively, locations of any recovery sites and what the facilities allow may be set out. This can include information on:

- capacity
- parking
- welfare
- post
- meeting rooms
- disabled access
- access for employees
- transport.

Phased return to operations
This plan sets out how quickly normal service delivery can be resumed following issues requiring the plan to be invoked. This outlines what functions should be up and running within a certain timeframe. Contractual and legal requirements will take precedent followed by the services that are required to support them.

Step eight - equipment and resources
This sets out what equipment is required either in order to work from home, or from an

alternative location, and how soon it should be made available, including the number of workstations, any hardware and access to software applications.

Further considerations may be outlined within this section, including:

- diversion of telephones
- connectivity
- stationery
- back up processes
- documentation and records etc.

Step nine - testing
We will implement a plan for testing all elements of the Business Continuity Management Plan.

It will break down each element and ensure that the individual components can be mobilised, this may be broken down into role plays, desktop exercises and full drills.

Key Response Personnel

Inga Andries (Managing Director) 07432 130095
i.andries@trinityharpercleaning.co.uk

Paul Prime (Business Development Director) 07542 683547
p.prime@trinityharpercleaning.co.uk

Barry Nicholls (Operations Manager) 07885 459463
b.nicholls@trinityharpercleaning.co.uk

Rachel Loughney (Administrator – Sales/Purchase Ledger)
r.loughney@trinityharpercleaning.co.uk

Chelsea Finn (Administrator – Payroll)
c.finn@trinityharpercleaning.co.uk

James Bee (Cambridge Network Solutions) 07709 253514
James.bee@cambridgenetworksolutions.co.uk

Risks and Responses

RISK	POTENTIAL EFFECT	IMMEDIATE ACTION	BY WHOM	LONGER TERM ACTION	BY WHOM
Office premises incapacitated due to fire, flood, burglary or vandalism.	1. Loss of power including internet. 2. Loss of computer hardware including printer. 3. Loss of paper files and records.	1. Inform all 'office' based staff to work from home. 2. Evaluate losses and immediate needs, purchase replacements. 3. None required, all files are stored and backed up in the Cloud.	1. Inga Andries/ Barry Nicholls/ Paul Prime 2. Inga Andries/ Barry Nicholls/ Paul Prime 3. N/A	1. Communicate with Landlord and Insurers. Ascertain extent of damage and evaluate potential need for temporary and/or longer-term replacement accommodation. 2. N/A 3. N/A	1. Inga Andries 2. N/A 3. N/A
Cyber attack	1. Loss of access to electronic data. 2. Loss of access to electronic banking.	1. Contact James Bee at Cambridge Network Solutions for advice and assistance. 2. Contact James Bee at Cambridge Network Solutions for advice and assistance.	1. Inga Andries/ Paul Prime. 2. Inga Andries/ Paul Prime.	1. Evaluate and improve electronic security measures. 2. Evaluate and improve electronic security measures.	1. Inga Andries/James Bee. 2. Inga Andries/James Bee.

Signed Date: 11th January 2025

Inga Andries (Joint Managing Director)