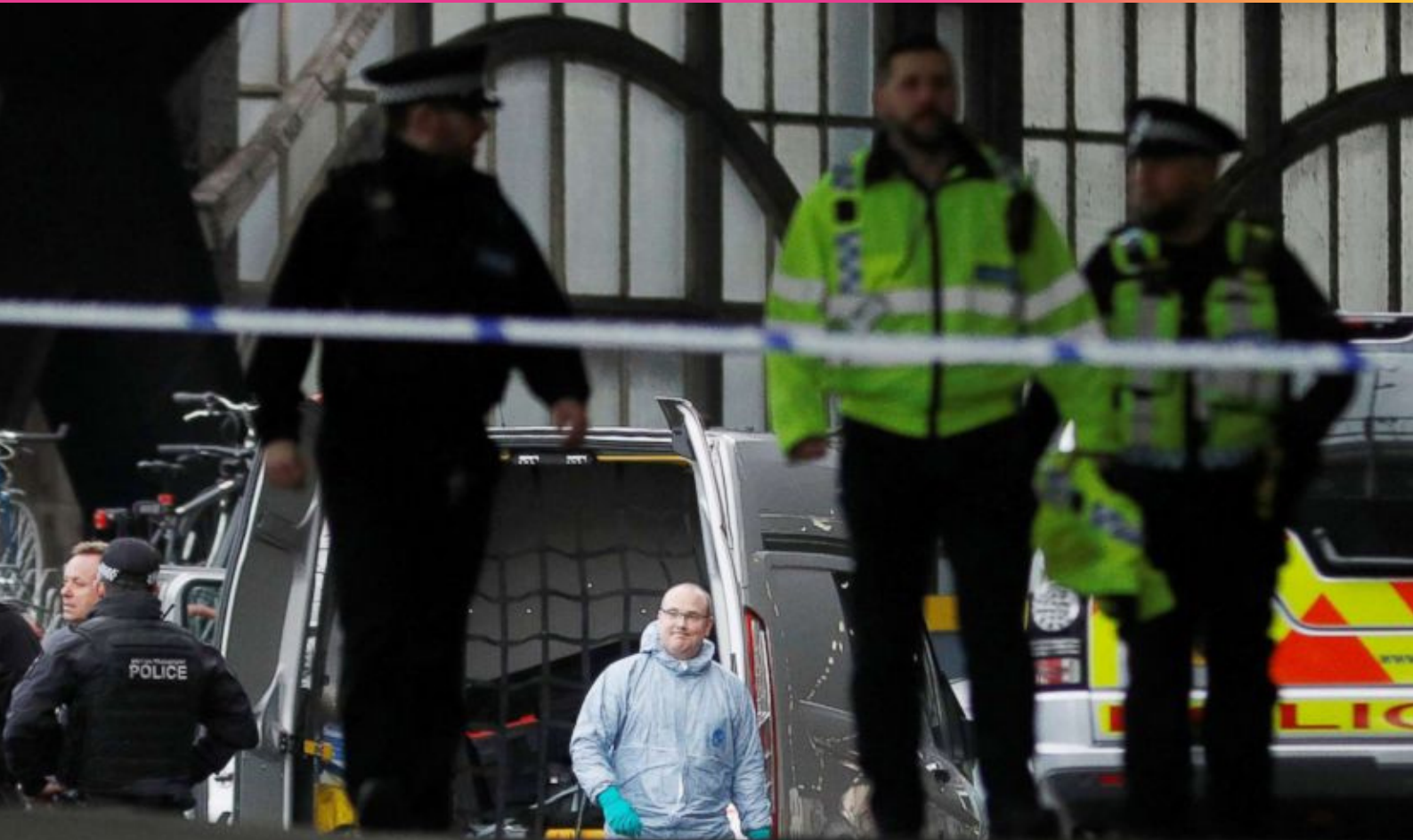# WEAREWATERLOO

BUSINESS CONTINUITY PLAN TEMPLATE

ABOUT THIS BUSINESS CONTINUITY PLAN TEMPLATE

Please keep this document somewhere safe on site. A second copy should be kept off-site at a safe and secure location. This document should be reviewed and updated on an annual basis.

Disruptive incidents can take many forms and can happen at any time. Many of these are localised and can be due to to infrastructure failures (such as the flooding at Southwark Tube in Jan 2020, shown above), crime scenes which cover large areas (including Lower Marsh in Dec 2022) or cautionary area cordons (including the Waterloo Station postal bomb scare in Mar 2019). All of these and more cause business operations to be disruptive and premises inaccessible.

The objective of this plan is to facilitate the swift recovery of business operations after a disruptive incident.

Contents

This document has been compiled by WeAreWaterloo Business Improvement District in collaboration with the Metropolitan Police Counter Terrorism Protective Security Operations department. The information contained within this document is suggested advice only. No part of it should imply that the information is a guarantee or insurance against any major disruptive incidents and serves to highlight potential issues that may occur and ways in which they can be prepared for.

This section contains the contact details for persons that are essential for continuing the operation of the organisation.

Name	Job title	Mobile Number	On site?

02   COMMAND CONTROL

The decision to use this plan will be taken by the named GOLD command, who will also be responsible for taking the "difficult" decisions for the organisation overall. Often the business manager or security manager will be expected to take charge, but what if they are not available because of the incident? Who else can be delegated responsibility?

Many companies have fire wardens within their organisation, this can be extended to have staff empowered and ready to deal with other incidents as well.

Name	Title	Mobile No.
	GOLD	
	SILVER	
	BRONZE	

Waterloo, London, UK

What are the most likely threats to your business, is a terrorist attack your main concern or is it loss of IT or general crime? What is more likely to impact your business and what can you do to minimise the risk? Analyse the risk by asking yourself the following questions: How can you cope with it i.e. what do you need to do to stay operational if it takes place? What preventative measures can you take to prevent them from happening or minimise the effect they will have on your business? Are you insured against the worst eventualities?

Threat to business	Severity of Impact	Assets Affected	Likelihood	Mitigation Measures

What are the main functions of your business? What actually needs to be done and in what order? List what functions need to take place.

This list may be used as a checklist to ensure that critical tasks are completed on time and according to a pre-agreed priority schedule.

It may also be used to provide a handover document between different shifts in the recovery process.

Priority	Critical Function	Recovery Length

Following from the critical function checklist, what are those key functions that need to be done and who will be responsible for each one. Who will: open/close the premises, start up/shut down the computers or machinery, backup the essential data, contact staff members, contact suppliers, organise orders or bookings, arrange invacuation/evacuation, follow ups with staff once safely away from the incident. These are just examples and every business is different, a pub will have different priorities from a large office. What are the critical functions you need to have completed and by whom?

Critical Function:	
Responsiblilty:	
Recovery timeframe:	
Likelihood:	
Staff required for recovery:	
Data assets required for recovery:	
Premises required for recovery:	
Supplies required for recovery:	
Equipment required for recovery:	
Communications required for recovery:	

Following from the critical function checklist, what are those key functions that need to be done and who will be responsible for each one. Who will: open/close the premises, start up/shut down the computers or machinery, backup the essential data, contact staff members, contact suppliers, organise orders or bookings, arrange invacuation/evacuation, follow ups with staff once safely away from the incident. These are just examples and every business is different, a pub will have different priorities from a large office. What are the critical functions you need to have completed and by whom?

Critical Function:	
Responsiblilty:	
Recovery timeframe:	
Likelihood:	
Staff required for recovery:	
Data assets required for recovery:	
Premises required for recovery:	
Supplies required for recovery:	
Equipment required for recovery:	
Communications required for recovery:	

Following from the critical function checklist, what are those key functions that need to be done and who will be responsible for each one. Who will: open/close the premises, start up/shut down the computers or machinery, backup the essential data, contact staff members, contact suppliers, organise orders or bookings, arrange invacuation/evacuation, follow ups with staff once safely away from the incident. These are just examples and every business is different, a pub will have different priorities from a large office. What are the critical functions you need to have completed and by whom?

Critical Function:	
Responsiblilty:	
Recovery timeframe:	
Likelihood:	
Staff required for recovery:	
Data assets required for recovery:	
Premises required for recovery:	
Supplies required for recovery:	
Equipment required for recovery:	
Communications required for recovery:	

09   EMERGENCY RESPONSE

This is a template for what you should consider doing as a part of your emergency response; creating a log will keep you organized and focused on the priorities during an incident. Think how you will brief staff, where you will be and does everyone know what they need to do?

Within the first 24 hours

Task	Completed by and time
Start a log of all actions taken and expenses	
Liaise with emergency services (see section 15)	
Identify & quantify damage e.g. staff, premises, data, records	
Assess and action key priorities as per the Critical Function Checklist	
Provide information to staff, suppliers, customers & insurance	

Daily & Ongoing Actions

Task	Completed by and time
Convene those required to action Critical Functions	
Keep staff, suppliers, customers and insurance aware of updates	
Outline necessary information publicly to maintain reputation	
Assess and action key priorities as per the Critical Function Checklist	
Provide information to staff, suppliers, customers & insurance	

10 GRAB BAG CONTENTS

As part of the recovery plan for the organisation, key documents, records and equipment are held in a grab bag. This pack may be retrieved in an emergency to aid in the recovery process. It is important the robust grab bag is reviewed monthly and kept fully stocked. A second bag should be securely located off-site, in the event that the primary premises are inaccessible. The bags should comprise of the following:

Documentation:
- Emergency evacuation plan
- Business continuity plan
- Staff list (including next of kins)

Health and Safety:
- Hi-Vis Vests
- Torches (wind-up)
- Enhanced first aid kit
- Baby wipes

Communication:
- Laptop & spare phones
- Loudhailer & Radio (battery operated)
- USB drives (with critical information)
- Notebook & pencils (to document decision making)

Other:
- Petty Cash
- Spare keys
- Bank cards & pin sentry

11 KEY SUPPLIERS

Remember that you are likely to be a customer and will have suppliers that you may rely upon. Record the list of suppliers that you will need to contact in a crisis to either cancel, redirect or postpone deliveries from. Also if an incident affects not just you but your suppliers, you may want to have an alternative in mind.

Supplier	Provides	Telephone	Email

If you are evacuated, you won't have time to complete your important customer order or send a vital email. How will you contact those key customers to make them aware of the situation? They will appreciate you thinking of their needs and that will help them make alternative arrangements. Keeping them informed will help keep them as customers when things have returned to normal.

Customer	Receives	Telephone	Email

13   UTILITIES & FINANCE COMPANIES

Utility/Service	Company	Telephone	Email
Gas			
Water			
Internet			
Phone			
Electricity			
Banking			
Insurance			

15   EMERGENCY CONTACTS

Service	Website	Telephone
Emergency services		999
British Transport Police	btp.police.uk	0800 40 50 40
NHS	111.nhs.uk	111
Anti-Terror Hotline	met.police.uk/tua/tell-us-about/ath/possible-terrorist-activity	0800 789 321
Non-emergency police	met.police.uk	101
Floodline	check-for-flooding.service.gov.uk	0845 988 1188
Transport for London	tfl.gov.uk	020 7222 1234

16   USEFUL WEBSITES

Protect UK

ProtectUK provides vital information, official guidance and leading advice, helping you to detect vulnerabilities, connecting you with the best resources and helping businesses and individuals protect their staff, customers and location. ProtectUK has been developed by the Counter Terrorism Alliance, a focussed collaboration of three leading organisations: NaCTSO, Homeland Security Group (Home Office) and Pool Reinsurance.

Protect UK is best accessed via their app.

Twitter
We strongly advise following the accounts outlined below:
- @MetPoliceUK
- @BTP
- @LondonProtect
- Your local metropolitan neighbourhood team(s)