Business Continuity Plan Templates & Checklists

Business Continuity Documents	Yes/ No	Owner/ICO	Action/ Comment
Site and building security checklist			
Site plan			
Business Continuity plans			
Communications Plan			
Short-term loss or shortage of staff or skills plan			
Premises / facilities			
Technology			
Suppliers and Contractors			
Evacuation plan			
Bomb Alert plan			
Shelter (Invacuation) plan			
Lockdown plan			
Post Incident Support Checklist			

Staff	Contact Information

Insurance Providers	Contact Information

Other Useful Contacts	Contact Information

Also consider using grab and go emergency response boxes which contains useful information, including your plans, and emergency resources such as first aid kits, torches, pen and paper, etc.

Business Continuity Actions Checklist

Business Continuity Actions	Completed (sign date)	Comments / Further information
Invoke the relevant emergency action plan, i.e. evacuation and deal with the immediate emergency/incident		
Undertake post incident support activities and evaluate the impact of the incident		
Consider:		
Which department activities are disrupted?		
What is the impact of these activities being disrupted?		
Are there any critical activities approaching?		
Plan how critical activities will be maintained (using your Business continuity plans below) giving consideration to:		
Immediate priorities.		
Communication strategies		
Deployment of resources		
Finance		
Monitoring the situation		
Reporting		
Stakeholder engagement		
Log all decisions and actions, including what you decide not to do and include your decision making rationale		
Log all financial expenditure incurred		
Complete a lessons learnt log, what went well? What didn't? (see debrief and lessons learnt)		
Complete a post incident review		
Implement any improvements or findings, such as:		
Do emergency action plans need updating/ enhancing?		
Do policies need amending?		
Are building improvements necessary?		
Are there any training and development needs?		

Communication Checklist

As a result of an incident you may be unable to access your premises and access to resources may be limited. Consideration should be given to how you will be able to access information remotely. In the worst case scenarios it may not be possible to retrieve any information from the site. Consideration should be given to securely storing copies of information offsite.

Communications Plan Checklist	Yes/ No	Comment
Can you remotely access contact details of:		
Staff		
Local Authority		
Utility Companies		
Suppliers		
Contractors		
Insurance companies		
Do you have remote access to issue communications?		
Update website		
Social Media		
Email		
Text		
Incident Information Line		

Staffing Checklist

Managing short-term loss or shortage of staff or skills	Yes/ No	Comment/Action
Do you have deputies for all management and incident roles?		
Can you multi / cross skill staff?		
Consider different ways of working, such as:		
Home working		
Temporary alternative office space		
Consider alternative resourcing, such as:		
redeploy staff from other roles		
recruit temporary staff		
staff from other stores/offices		
Is short-term closure necessary?		

Premises / Facilities Checklist & Template

In the event of an incident the owner / manager will need to consider if the facilities are safe and fit for purpose, seeking advice from the emergency services and or other experts such as health and safety advisors, structural engineers, electricians etc. If the premises are considered unsafe then they should be closed and secured until remedial action is complete.

Managing Partial Closure
Isolate and secure the affected areas to prevent unauthorised access and display relevant warning signs
Consider different ways of working (as listed above)
Consider sourcing additional facilities such as modular buildings, portable toilets, generators, lighting etc
If not, can anyone help?
Have you pre-agreed arrangements with other premises in the community i.e. leisure centre, community centre, town/village hall?
If not, can anyone help?

Managing Total Closure
Secure premises to prevent unauthorised access and display relevant warning signs
Display details of where people can find information about the closure, advice and contact information

Potential Suppliers	Contact details	Comments
Modular buildings / Portable toilets		
Power generators / Lighting		
Boarding / Glazing providers		
Security		
Logistics / Transport		
Other		

Alternative premises in the event that it is considered necessary to close or partly close the premises	
Name of venue	
Type of venue	
Contact name	
Contact telephone number	
Useful info such as distance from premises, directions, capacity, opening hours	

Technology Checklist

Network / IT failure	Comments /information
Is essential business data backed up off site?	
Is essential business data kept on paper file?	
Do you have secure cloud based services?	
Do you have laptops/tables that can work offline?	
Do you have paper contingencies for record keeping, such as rota's, accident forms etc?	
Can you revert to paper based activities?	
Do you have a data recovery plan?	
Can you forward calls to a mobile?	

IT and Telephony Suppliers	Contact information
Line faults	
Network Supplier	
IT support	
Mobile phone	
Other	

Suppliers & Contractors Template

Pre-identified alternative Suppliers / Contractors	Contact information

Site and Building Security Checklist

Whole Site Security	Yes/ No	Comment/ Action
Is the whole site protected by perimeter fencing?		
Can pedestrian access be limited / restricted? i.e. by locking gates		
Are there public footpaths?		
If so, are they fenced?		
Can vehicular access be limited / restricted? i.e. by locking gates and or bollards etc		
Is there CCTV?		
If so, is it: monitored?		
are notices/warnings clearly displayed?		
Do you have any security guards, or staff patrolling the grounds?		
Is the site overlooked?		
Is there a process for dealing with a security alert?		
Are there arrangements to enhance security if the situation becomes critical?		

Building security	Yes/ No	Comment/ Action
Are access points supervised?		
Are access points locked? i.e. can they only be accessed with a key/code?		
If so who has access to key/code? And is this monitored and maintained?		
Is there access between public and restricted areas?		
Are there any alarm systems (e.g. burglar alarms, panic alarms)		
Do all staff wear identification?		
Do you have procedures for visitors?		
Are unsupervised visitors / contractors etc signed in and issued with identification?		
Do all staff wear a uniform?		
Do all staff wear identification?		
Are people not wearing identification challenged?		
Is identification carefully checked?		
Are staff made aware not to allow tailgating by unknown visitors?		
Can windows be fully opened?		
Do you have an intruder / panic alarm?		
If so is it linked to the police and or a security company?		
Do staff have any other means of raising the alarm? i.e. mobile phones		
Is there a process for dealing with a security alert?		
Are there arrangements to enhance security if becomes critical?		