Business Continuity Plan

For

Disaster Recovery in the event of a Critical Incident

10/10/2024

Document Control

Title:	Business Continuity Plan
Client:	N/A
Reference:	
Classification	External
Version:	1.0
Release Date:	29/10/2024
Author:	James Cox
Total Pages:	16
Disclaimer:	This document is protected by copyright laws in England and other countries and must not be copied, stored in a retrieval system or transmitted in any form or by any means in whole or in part without the prior written permission of Bespoke IT Solutions Ltd.

Document Approval

Approved By:	Natalie Alden	Approved by e-mail

Revision History

Version	Date	Issued By	Status	Comments
0.1	10 Oct 24	J Cox	Draft	For review
1.0	10 Oct 24	J Cox	Final	

1.0 Introduction

Bespoke It Solution's ("BITS") Business Continuity Plan (BCP) has been written for those who will be involved in re-establishing the operational delivery of services following a major incident.
The purpose of the plan is to provide a flexible response so that BITS can:

- Respond to a disruptive incident (incident management)
- Maintain delivery of critical activities/services during an incident (business continuity)
- Return to 'business as usual' (resumption and recovery)

The Business Manager, BITS is this Plan's Owner and responsible for ensuring that it is maintained, exercised and updated in accordance with internal requirements for business continuity.

2.0 Definitions

An emergency is any event which causes, or has the potential to cause injury, loss of life, damage to property or significant business disruption.
A disaster is the escalation of an emergency to the point where normal conditions are not expected to be recovered for at least 24 hours.

3.0 General Information

BITS has adopted the ''Plan-Do—Check-Act'' PDCA model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of the organisation's Business Continuity Management system (aligned to ISO22301)
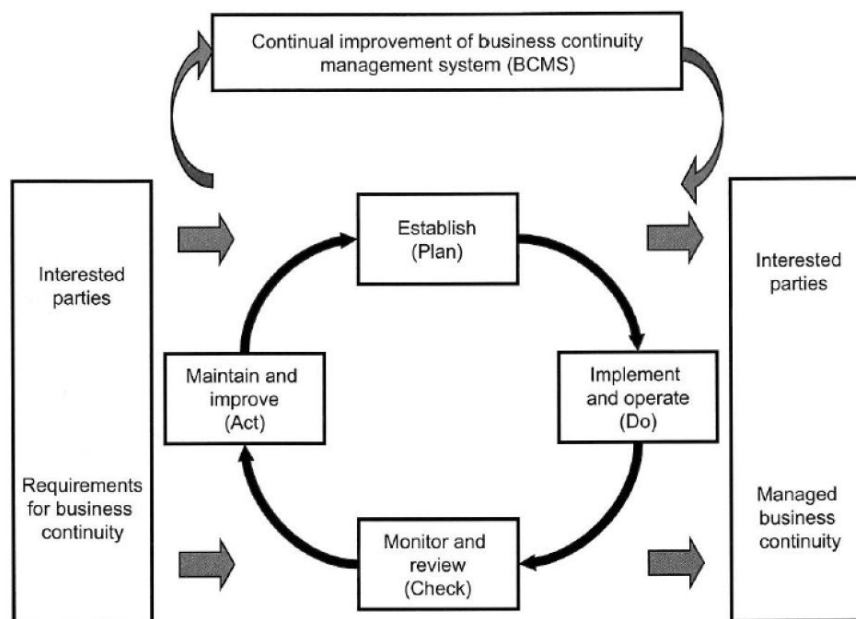
9.3   **Brief explanation of the PDCA model**

3.1 Review and Training

This document will be reviewed, evaluated and updated by the BITS Wider Management Team every year as well as whenever there are significant changes in personnel, equipment, operating software or recovery strategies.

Mechanisms for raising awareness include:
- involving staff in the development of the strategy;
- written and oral briefings;
- learning from internal and external incidents; and
- discussion based exercises

All new staff are made aware of the organization's BCP arrangements on joining and this forms an integral part of our induction process.

Characteristics of the Business Continuity Plan will be monitored and analysed where appropriate.
Monitored information includes:

(a) Reports on business continuity incidents that have invoked a formal response.
(b) Exercises completed (to help ascertain comprehensiveness).
(c) Business continuity plan audit checklists
(e) Internal audits will be planned, documented, undertaken and recorded. Identified non-conformity will be recorded within the audit report, and any required corrective actions implemented.

3.2 Associated Documents/information

The Business Continuity Plan should be read in conjunction with:
- Fire evacuation plan for Westmead House (the operation of which does not necessarily activate the BCP)
- Fire Risk Assessments
- Health and Safety Policy
- Information Security Policy
- Data Protection Policy
- Remote Working Policy
- Reporting a Security Breach, Incident or Vulnerability

3.3 Emergency Contact Information

An emergency information pack is kept **in the main office/on the intranet** and includes:
- Copies of this document
- Emergency contacts list

Access to all staff contact information (those currently active), data and business information can be accessed securely on-line through the Bamboo HR system to ensure business continuity at all times. Bamboo is secure and cloud based and backed up online on a hosted server (in the cloud). In addition, BITS business model is based on using cloud-based services and is focused on staff and contractors being able to work from any location with full access to all operational tools and resources. This enables remote working with an Internet connection and cuts out many of the on-site potential disaster risks (fire, flood, loss and damage of physical storage media).

4.0   Strategy and Plan Activation

A business continuity incident is an event or occurrence that disrupts, or might disrupt, normal service delivery below acceptable predefined levels, where special arrangements need to be implemented until services can return to an acceptable level.

The purpose of this Business Continuity Plan (BCP) is to provide the internal framework to prepare for, respond to and recover from business and service disruption irrespective of the cause.

This Plan will be activated in response to an incident causing significant disruption to normal service delivery/business, particularly the delivery of key/critical activities. Examples of circumstances triggering activation of this Plan include:

- Loss of key staff or skills e.g. above normal levels of absenteeism due to illness
- Loss of critical systems e.g. ICT failure
- Denial of access, or damage to, facilities e.g. loss of a building through fire
- Loss of a key resource e.g. a major supplier vital to the delivery of a key service
- Notification of a Pandemic or national incident

Staff communication will be via email, MS Teams and What's App or by use of the telephone lists if not.

The following organisations may need to be advised of the implementation of the Business Continuity Plan as soon as possible:

- Contractors
- Crown Commercial Services
- Existing private contract key stakeholders
- All public sector contract key stakeholders
- Insurance Advisors
- Sub-contractors
- Accountants
- IT Partners

5.0   Roles and Responsibilities

5.1   Business Manager or a member of the management team

The Business Manager is responsible for the implementation and co-ordination of the BCP, including:
- Immediately contacting the Landlords if the disaster relates to the built environment or the ICT infrastructure to establish if the building can be re-occupied and/or service delivery reinstated
- Co-ordination of status reports/communication for the benefit of all audiences (including staff, temporary workers, contract stakeholders, framework providers and subcontractors)
- Maintaining the BCP in an up-to-date format by delegating responsibility to the Quality Co-ordinator for updates.

5.2   Incident Management Team (IMT)

Lead by the Business Manager or member of the management team, the Incident Management Team includes all members of the Wider Management Team. Additional members of the team will be recruited to match the specific needs of the incident.

The IMT is responsible for acting under the direction of the Business Manager (or their Deputy) to restore normal conditions as soon as possible.

Purpose of the Incident Management Phase

- Protect the safety of staff, visitors and the wider community
- Protect vital assets e.g. equipment, data, reputation etc.
- Ensure necessary communication takes place
- Support the Business Continuity phase
- Support the Recovery and Resumption phase

5.3   Staff

Staff are required to co-operate with the IMT in support of the BCP.
In the event that staff are sent home, they should remain available during normal working hours to assist with necessary tasks.

6.0   Evacuation of Premises and Safeguarding of Staff

Action	Details
Evacuate the building if necessary	Use normal evacuation procedures for the building
Call emergency services (as appropriate)	TEL: 999 Business Manager or delegate is responsible for completing this action
Person on-site to notify manager	Do not enter the building
Check that all staff, contractors and any visitors have been evacuated from the building and are present. Consider safety of all staff, contactors and visitors as a priority	All visitors are required to sign in at reception, the fire wardens in our office have a responsibility to ensure that all staff and visitors are assembled.
Alert staff	Alert any staff due to arrive on-site soon of the incident, and tell them to await further instructions
Ensure log of incident is started and maintained throughout the incident phase	Incident log template can be found on the Intranet under Internal HR Documents/Health and Safety
Record names and details of any staff, contractors or visitors who may have been injured or distressed in the incident.	Business Manager or delegate is responsible for completing this action

Forward details of any fatalities or injuries in the incident to our HR partner (depending on scale of incident) and agree action that will be taken.	The Business Manager will forward this information to Vivo HR
Assess impact	Senior management team meet to assess the scale of the incident & decide next steps
Consider whether the involvement of other teams, services or organisations are required to support the management of the incident	Depending on the incident the following may be approached to assist with incident management: • Health and Safety/Occupational Health

6.2   Closure during a Business Day
It is never a preferred option to Interrupt any planned delivery, but it can be done using the following procedures:
1. Cancellation authorised by the Duty Manager or deputy
2. Communications will be made with relevant customers should we close.

6.3   Immediate Places of Safety
In the event of a major incident on or off site requiring normal operations to be closed, staff will assemble at the primary assembly points. If these are not useable identified staff will escort all workers to the secondary assembly points.

6.4   Off-Site Place of Safety
If it becomes necessary to evacuate the site completely, staff and workers will be escorted to the identified place of safety in accordance with local procedures.

7.0   Lockdown Procedure

It is now possible to envisage circumstances where the business may wish to lock itself in, to secure staff and workers from an outside threat. This circumstance is described as a 'lockdown'.

If a lockdown is declared:
- BITS Duty Manager will be advised to implement the lockdown via word-of-mouth or by using mobile telecommunications.
- The SMT will communicate via Telephone and text
- The business will be advised that it is in 'lockdown' by word-of-mouth
- All staff will remain in training rooms and offices and keep workers calm and away from windows

8.0   Silent Evacuation

Should there be a need for a silent evacuation, staff will be notified by email or MS Teams. They should evacuate the building to the Bespoke IT Solutions designated assembly point in

front of Hobby Craft. Staff should familiarise themselves with the procedures on customer site.

9.0 Business Recovery in the Event of a Loss of Buildings or site Space

9.1 General
Replacement of the buildings and facilities that have been damaged or made unavailable will be the responsibility of the Landlord.

Temporary working facilities are the responsibility of BITS for which it holds insurance (see below).

9.2 Insurance
BITS hold insurance of sufficient value to cover the cost of temporary accommodation.

9.3 Replacement Site Facilities
The size and scope of facilities required for the business will vary according to circumstance. In the first instance contact should be made with the Insurance. As the BITS business model is based on using cloud services and is focused on staff and contractors being able to work from any location with full access to all operational tools and resources, it is unlikely that alternative accommodation will be needed for the majority of staff. However, we may wish to source alternative accommodation for our Help Desk team.

The location of the temporary accommodation will be determined based on the space required and circumstances at the time or staff will be directed to work remotely from home.

Business Continuity

Critical activity	Details	Responsible Person(s)
Plan how critical activities will be maintained.	Consider: ▪ Immediate priorities ▪ Communication strategies ▪ Deployment of resources ▪ Finance ▪ Monitoring the situation ▪ Reporting	Incident Management Team ("IMT")
Identify any other staff required to be involved in the BC response	Depending on the incident, the Business Continuity Team may need additional/specific input in order to drive the recovery of critical activities	IMT
Log **all** decisions and actions, including what you decide **not** to do and include rationale	Use a decision and action log to do this	IMT
Take any salvage/asset recovery actions that are appropriate	Remove any equipment, furniture, and records etc that are at risk of damage.	IMT

Critical activity	Details	Responsible Person(s)
Continue to log all expenditure incurred as a result of the incident	Use a financial expenditure log to record costs incurred as a result of responding to the incident	Business Manager
Insurance	Inform insurance company	Business Manager
Landlord	Inform Landlord	Business Manager
Post redirection	Form available on company intranet	Office Manager
Inform all key stakeholder customers	If disruption is expected, inform all key stakeholders via email	All Staff directed co-ordinated by Manager- ensure regular updates are provided in relation to business continuity
Evaluate the impact of the incident	Use an incident impact assessment form to understand the impact of the incident on 'business as usual' working activities.	IMT

Infrastructure incident

An infrastructure incident can include the loss of computer / telephony systems, internet access, or power.

Step 1: Understand the extent of the loss

Infrastructure	Details	Responsible Person(s)
Phones	Contact phone provider to ascertain extent of outage.	Technical Manager
Internet	Contact internet provider to ascertain extent of outage.	Technical Manager
Mains power	Contact power provider to ascertain extent of outage.	Technical Manager

If outage is temporary, inform staff to stay put and await further instructions. If the outage is ongoing:

Step 2: Business continuity

Critical activity	Details	Responsible Person(s)
Phones	Staff to use personal mobile phones. Contact telephone provider to forward office lines to staff mobiles	Technical Manager

Internet	Staff to use home internet connections. If home connection unavailable contact local shared office providers to rent desk space	Line Managers
Mains power	Staff to work from home until power is restored. If power outage is widespread and staff homes are also affected contact local shared office providers to rent desk space.	Line Managers

Staff incident
A staff incident can include a sudden family emergency, injury or other event which renders a key member of staff suddenly unable to work.

Step 1: Ensure no service interruption

Critical activity	Details	Responsible Person(s)
1. Identify interchangeable staff	All members of staff should have team members who can perform their roles, even if it is in a reduced capacity. Identify the relevant person and support them in carrying out business-critical activities	Line Managers
2. Assess extent of loss	Identify whether the affected staff member's absence is likely to be temporary, longer-term, or permanent. Keep in mind this may be a difficult period for the staff member and / or their family.	Line Managers

If the staff loss is temporary, support the member of staff who will be filling the gap until the absent member of staff returns. If the absence is long-term or permanent:

Step 2: Business continuity

Critical activity	Details	Responsible Person(s)
1. Recruit temporary or full-time replacement	Follow the standard recruitment procedure to find a full-time, part-time or fixed-term contract (as appropriate) replacement.	Line Manager

Recovery phase

The purpose of the recovery phase is to resume normal working practises for the entire organisation. Where the impact of the incident is prolonged, normal operations may need to be delivered under new circumstances e.g. from a different building.

Action	Details	Responsible Person(s)
1. Agree and plan the actions required to enable recovery of normal working practises	Agreed actions will be detailed in an action plan and set against time scales with responsibility for completion clearly indicated.	Senior Management Team
2. Respond to any long term support needs of staff	Depending on the nature of the incident, we may need to consider providing support services	Wider Management Team
3. Publicise that there is now 'business as usual'	Inform customers through normal channels that our business is operating as normal	Wider Management Team
4. Carry out a debrief of the incident and complete report to document opportunities for improvement and any lessons identified	This should be reviewed to ensure key actions resulting from the incident are implemented within designated time scales.	Senior Management Team
5. Review this Continuity Plan in light of lessons learned from incident and the response to it	Implement recommendations for improvement and update this plan. Ensure a revised version of the plan is read by all members of staff.	Wider Management Team

10.0   Pandemic Threat / Mass Staff Unavailability

Loss of staff is considered a generic threat to operations. The spread of a virus capable of impacting on operational service delivery is now considered genuine and serious.

In the event of mass staff illness, the SMT will shut the business to all staff, visitors and temporary workers.

Current Risk Assessment in relation to Covid-19

Provider	Bespoke IT Solutions Ltd	
Venue(s)	Any office, venue, facility, vehicle that we utilise will be risk assessed with control measures put in place to mitigate risk in line with latest Government Covid-19 guidance.	
Hazard	Coronavirus (COVID-19)	
Persons who can be harmed	Employees Non-employees Temporary Workers Visitors	*Clinically extremely vulnerable* people – those who have received a letter from the NHS advising them to 'shield'

	Contractors (Consideration must also be given to disabled people in the above groups)	*Clinically vulnerable* people – those who are either pregnant or who have underlying health conditions
How people can be harmed	Inhalation of water droplets from people who have COVID-19. The droplets can be dispersed by coughing or sneezing. They are also released during breathing, so the droplets can be inhaled by others standing in close proximity. The water droplets can also land on surfaces and be subsequently transferred by touching these infected surfaces then touching the mouth, nose or eyes	
Level of risk	The risk of contracting the virus is variable according to the following factors: - The prevalence of the virus in the community - The interaction of people with others i.e. the *number* of people an individual encounters and the proximity of such contact - The likelihood of touching contaminated surfaces and transferring the virus to the mouth/nose/eyes The severity of harm from the virus will depend on the following factors: - If the individual is clinically extremely vulnerable or clinically vulnerable - If the individual is pregnant - The age of the individual	
Control Measures	Control measures are those systems and physical controls which will reduce the risk of contracting the virus. The most effective control measure is to work from home. Where this is not possible, maintain a 'social distance' of at least 2m from any other person which will reduce the risk of inhaling water droplets. Individuals should avoid confined spaces (e.g. lifts, small interview rooms etc) where possible. Limiting the *number or people* an individual encounters will reduce the risk of transmission of the virus (called 'fixed teams' or 'partnering'). Reducing the amount of *time* that individuals are in contact with others will also reduce the risk. The layout of workplaces to prevent staff facing each other will reduce the risk of inhalation of droplets. The use of Perspex screens will reduce the risk of droplets being transferred from one person to another where staff are in close proximity Limiting contact with common areas (i.e. meeting rooms, kitchens, hot-desks) will reduce the risk of touching contaminated surfaces Regular hand-washing with soap and water is an effective way of removing the virus from the hands. Regular cleaning of surfaces, handles, handrails etc will reduce the risk of the virus surviving on surfaces. DIY cleaning (i.e. staff cleaning their own work-stations) will reduce the risk of touching contaminated surfaces	

11.0   Other Threats Incident and Threat Types

The following Other Threats have been considered
- Finance Process Breakdown – payments to staff & suppliers fail
- Key Supplier Failure other than Company Name– Catering, transport
- Evacuation due to Nearby Incident
- Bad Weather prolonged
- Strikes

Risk assessment

Company name: Bespoke IT Solutions Ltd

Assessment carried out by: Steve Newton

Date of next review: 09/10/2025

Date assessment was carried out: 10/10/2024

What are the hazards?	Who might be harmed and how?	What are you already doing to control the risks?	What further action do you need to take to control the risks?	Who needs to carry out the action?	When is the action needed by?	Done
Slips and trips	Staff and visitors may be injured if they trip over objects or slip on spillages.	General good housekeeping. • All areas well lit, including stairs. • No trailing leads or cables. • Staff keep work areas clear, e.g. no boxes left in walkways, deliveries stored immediately. • Offices cleaned every evening.	Excellent housekeeping in staff kitchen needed, e.g. on spills.	All staff, Line Managers to monitor	Ongoing	
Manual handling of paper, office equipment etc	Staff risk injuries or back pain from handling heavy/bulky objects, e.g. deliveries of paper.	Trolley used to transport boxes of paper and other heavy items when collecting deliveries etc. • High shelves for light objects only	Remind staff that they should not try to lift objects that look or appear too heavy to handle.	Line Managers	Ongoing	
Stress	All staff could be affected by factors such as lack of job control, bullying, not knowing their role	• Staff understand what their duties and responsibilities are. • Staff can talk to supervisors or manager if they are feeling unwell or at ease about things at work. • 'No bullying' policy.	Remind staff they can speak confidentially to their manager or supervisors if they are feeling unwell or ill at ease because of work	Line Managers	Ongoing	
Electrical	Staff could get electrical shocks or burns from using faulty electrical	Staff trained to spot and report (to office administrator) any defective plugs, discoloured sockets or damaged cable/equipment.	Ask landlord when the next electrical installation safety check is due.	Office Manager	Ongoing	

14

What are the hazards?	Who might be harmed and how?	What are you already doing to control the risks?	What further action do you need to take to control the risks?	Who needs to carry out the action?	When is the action needed by?	Done
	equipment. Electrical faults can also lead to fires.	• Defective equipment taken out of use safely and promptly replaced. • Staff told not to bring in their own appliances, toasters, fans etc.	• Confirm the system with landlord for making safe any damage to building installation electrics, eg broken light switches or sockets			
Fire	If trapped, staff could suffer fatal injuries from smoke inhalation/ burns	Working with landlord, fire risk assessment done, see www.fire.gov.uk/workplace+safety/ and necessary action taken.	Ensure the actions identified as necessary by the fire risk assessment are done.	Office Manager	Ongoing	
Lone working	Staff could suffer injury or ill health while out of office, e.g visiting clients' offices, or while working alone in the office.	Staff record visit details in office diary and give a contact number. • Staff not returning to the office after a visit call in to report this. • Security staff check all areas, including toilets, before locking up at night.	Whereabouts of staff 'out of the office' to be monitored by office based staff.	Line Managers/Team Leaders	Ongoing	
Display screen equipment	Staff risk posture problems and pain, discomfort or injuries, eg to their hands/ arms, from overuse or improper use or from poorly	DSE training and assessments of workstation carried out by all new starters. Actions carried out asap. • Reassessment to be carried out at any change to work feature, eg equipment, furniture or the work environment such as lighting.	Supervisors to monitor to ensure staff continue to get breaks away from the computer	Team Leaders	Ongoing	

What are the hazards?	Who might be harmed and how?	What are you already doing to control the risks?	What further action do you need to take to control the risks?	Who needs to carry out the action?	When is the action needed by?	Done
	designed workstations or work environments. Headaches or sore eyes can also occur, eg if the lighting is poor.	• Workstation and equipment set to ensure good posture and to avoid glare and reflections on the screen. • Shared workstations are assessed for all users. • Work planned to include regular breaks or change of activity. • Lighting and temperature suitably controlled. • Adjustable blinds at window to control natural light on screen • Noise levels controlled. • Eye tests provided when needed, duty holder to pay for basic spectacles specific for regular users of visual displays. • Laptop users trained to carry out own DSE assessment for use away from office. When used at office, laptop should be used with docking station, screen, keyboard and mouse.	Check that identified actions from self-assessments are followed up ASAP.	H&S Manager	Ongoing	
			Tell staff that they are to inform their manager of any pain they have that may be linked to computer use.	All staff	Ongoing	
			Remind laptop users to carry out regular DSE assessment to avoid problems and identify any issues.	H&S Manager	Ongoing	