[Your Company Name]

Business Continuity Plan Template

DOCUMENT AUTHOR:	[Insert Author]
DOCUMENT OWNER:	[Insert Owner]
STATUS:	[Draft/Approved]
DATE CREATED:	[Insert Date]
VERSION:	[Insert Version]
LAST UPDATED:	[Insert Date]
SECURITY CLASSIFICATION:	[High/Medium/Low]

Document Customisation

This page *(to end of the 'disclaimer')* provides template guidance and ***must be removed*** from the finished version. For information on customising this template, please refer to the *'Instructions'* supplied with your order.

It is important to work through the document and customise any areas to ensure that the finished template accurately reflects what your organisation does and the controls that you have in place. You should consider your regulatory and legal obligations and any standards or requirements that apply to your industry or business type when customising the content.

Template Guidance

We have provided a generic template as a starting point for you to develop your own document in this compliance area. You should review and customise the template sections thoroughly to ensure that the finished version accurately reflects your organisations' controls and responsibilities.

Referencing Other Policies

We sometimes reference other policies in a template where relevant *(i.e. refer to Anti-Bribery & Corruption Policy in conjunction with AML).* Referenced documents are **only** included in your pack if you have ordered them separately or you have purchased a Toolkit or Bundle that includes them.

Licence Terms

Purchased documents are for use within the ordering company **only** and cannot be used, sold or transferred elsewhere without written permission from Know Your Compliance Limited. Please refer to the *'Instructions'* document for more information on our T&C's and licence options.

Disclaimer

Know Your Compliance Limited has created this template for you to use in developing and implementing your compliance program requirements. Whilst every reasonable care is taken to ensure that the content is relevant, compliant and up to date; it is **your responsibility** to ensure that the finished policy complies with any regulatory and/or legal requirements and standards.

It is important that you customise the content to suit your industry needs and business type. Know Your Compliance Limited makes no claims or guarantees about the compliance or adequacy of the template content and accepts no responsibility or liability for any loss, damage or expense incurred as a result of reliance on our documents. If you are unsure of your obligations, you should obtain legal or professional advice before publishing, using or relying upon your finished policy.

Revision History

VERSION	REVISION DATE	SECTION REVISED	REASON FOR REVISION	DESCRIPTION OF REVISION

Table of Contents

1 Plan & Distribution Access 5
2 Introduction 5
3 Policy Statement 6
4 Purpose 6
5 Scope 6
6 Objectives 7
7 Disaster Recovery Plan 7
7.1 Distribution List 7
7.2 Business Impact Analysis 8
7.3 Critical Functions & Processes Checklist 9
7.3.1 Critical Function Assessment & Recovery Process 10
7.4 Non-Critical Functions 10
7.5 Specific Disaster Scenarios 11
7.6 Recovery Contact Lists 13
7.6.1 Employee Contact List 13
7.6.2 Key Suppliers Contact List 13
7.6.3 Key Customers Contact List 14
7.6.4 Utility Company Contact List 14
7.7 Office & Alternate Physical Locations 14
8 Emergency Pack 15
9 Updates & Annual Review 15
10 Actions and Expenses Log 15

Distribution list:

The distribution list should contain the names or all staff, locums or 3rd parties who have a copy of the BCP and who are aware of the procedures to be followed in the event of a crisis or emergency.

If you are a sole trader, it is still a regulatory and legal requirement that you have a working BCP and that at least one other individual or firm is aware of the BCP location and procedures.

1 Plan & Distribution Access

[Your Company Name]'s *(hereinafter referred to as the **"Company"**)* business continuity plan will be distributed to the relevant staff members of the business continuity and management teams*/locum or 3rd party firm*/nominated representative* [*DELETE AS APPLICABLE].

A master copy of this BCP document will always be maintained by the business continuity team leader or company owner and shall be located in a secure place off-site. For further risk mitigation, an electronic copy of this plan will be stored on a secure USB flash drive for printing on demand.

2 Introduction

Disaster Recovery (*or Business Continuity Planning*), is the processes, controls, measures, policies and procedures that together, enable a company to recovery and/or continue to trade following a natural or human-induced disaster or situation. All businesses should have some form of recovery program, however those in consumer credit and financial services industries are expected to have fully documented, robust and tested plans to protect consumer interests and safeguard assets.

Vital technology infrastructure and systems are susceptible to disruptions when dealing with potential threats and disaster recovery plans form an extensive program from documenting systems,

assets and information flows, through to stress-testing, back-ups and continuity plans. Any event that compromises or negatively impacts standard operations within the business are documented, with mitigating actions or alternative solutions included in the plan should a threat occur.

A plan will usually include a range of threats, risks and disasters that could happen, internal and external, natural or human-based, enabling Director and Senior Management to assess each scenario and implement measures and controls before the issue arises. It is essential in any Disaster Recovery Plan, to include all possible threats and risks and not just focus on the obvious ones such as fire, electricity outage or network issue. For example, if an illness or virus affected 50% of a business's workforce, to would be difficult to continue operating as normal or if the office location became uninhabitable, plans for back-up sites should be included.

3 Policy Statement

The Company's policy is to respond to any business disruption, emergency or crisis by safeguarding employees' lives and their property, mitigating risks to customers, continuing to comply with regulatory requirements, whilst making financial and operational assessments and quickly recovering and resuming normal business operations.

We are prepared for both internal and external disruptions in our BCP provision and will take every measure and precaution to ensure that any disruptions to our normal business function is mitigated against and prepared for. It is our aim that no customer is caused undue harm or inconvenience by any disruption that we may incur. Our recovery plan considers all possible threat and risk scenarios and details the appropriate measures and actions the Company has in place should they occur.

4 Purpose

The purpose of this policy is to provide a flexible and documented response so that the Company can respond to a disruptive incident, maintain delivery of critical activities and services during any such incidents and resume *'business as usual'* in the shortest time, with the least disruption.

This plan acts as a guidance and support document in the event of any threat scenario occurring and its development has included key stakeholder and prominent employees and suppliers.

5 Scope

The policy relates to all the Company staff *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas)* within the organisation and has been created to ensure that staff deal with the area that this policy relates to in accordance with legal, regulatory, contractual and business expectations and requirements.

6 OBJECTIVES

The Company is dedicated to restoring standard operating procedures as soon as is possible after any threat has occurred, and this recovery plan documents each aspect of the processes, measures and requirements to do that. ***We have several objectives for our recovery plan: -***

- To develop, retain and maintain a detailed and up-to-date Disaster Recovery Plan (DRP)
- Understand the critical functions and activities of the business
- Identify, analyse, assess and document risks to the Company and continued operation
- Identify the key roles, responsibilities and contacts to respond to an emergency
- Maintain effective running of the business in the event of a crisis or emergency
- To ensure that all staff are aware of the DRP/BCP and their role in complying with its processes
- To minimise disruptions to the Company's normal business operations
- To limit the extent and impact of any such disruption and/or damage
- To minimise the economic, client, customer and employee impact of any disruption
- To ensure that an alternative, adequate and appropriate means of operating is in place
- To ensure that employees and associated DRP/BCP suppliers are fully trained as to their part in any emergency procedure
- To provide a safe, swift and effective restoration to normal service

7 DISASTER RECOVERY PLAN

7.1 DISTRIBUTION LIST

The below distribution list contains the names, contact details and DRP role of any employee, lessee or 3rd party who has a copy of the DRP and who are fully aware of the procedures to be followed in the event of a crisis, threat or emergency.

This plan has been distributed to the relevant staff members of the business continuity and management teams and a master copy is maintained by the company Director and is in a secure place off site. For further risk mitigation, an electronic copy of this plan is stored on a secure USB flash drive for printing on demand.

NAME	TELEPHONE No	MOBILE No	POSITION

7.2 BUSINESS IMPACT ANALYSIS

The Company has completed a full ***Business Impact Analysis (BIA)*** and a risk assessment to enable us to understand our critical functions, risks to the continued operation of the business and plan for recovery. There are several key functions (*referred to in this document as Critical Functions*) that are essential to the normal operation of the Company and as such, require immediate restoration after an emergency incident.

LIKELIHOOD	IMPACT					
		Trivial (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
	Almost Certain (5)	Low Med	Medium	High	Very High	Very High
	Likely (4)	Low	Low Med	Med High	High	Very High
	Possible (3)	Low	Low Med	Medium	Med High	High
	Unlikely (2)	Low	Low Med	Low Med	Medium	Med High
	Rare (1)	Low	Low	Low Med	Medium	Medium
Impact Score x Likelihood Score = Risk Rating						

Function	Risk/Impact to Business	Risk Rating	RTO	Recovery Actions/Resources
E.g. Delivering services	*Unable to provide services, loss of clients, reputation damage*	*High*	*1 hr*	

Page removed from sample document

7.3.1 CRITICAL FUNCTION ASSESSMENT & RECOVERY PROCESS

The below assessment is completed for each critical function to ensure that it has a documented plan, recovery process, owner and timeframe.

Critical function	
Responsibility *(person/dept. responsible for leading on this function)*	
Potential impact/risk to organisation	
Recovery timeframe *(how quickly must this function be recovered to avoid lasting damage)*	
Staff required *(number, skills, knowledge, alternative sources)*	
Data / systems *(backup and recovery process, staff and equipment required)*	
Premises *(potential relocation or work from home options)*	
Communications *(methods of contacting staff, suppliers, customers, etc)*	
Equipment *(key equipment recovery or replacement processes)*	
Service Providers *(process to contact 3rd party service providers – gas, electric, water etc)*	

7.4 NON-CRITICAL FUNCTIONS

What are the essential, but non-critical functions of the business that must be restored within the first 4-8 hours?

Pages 11-15 removed from sample document