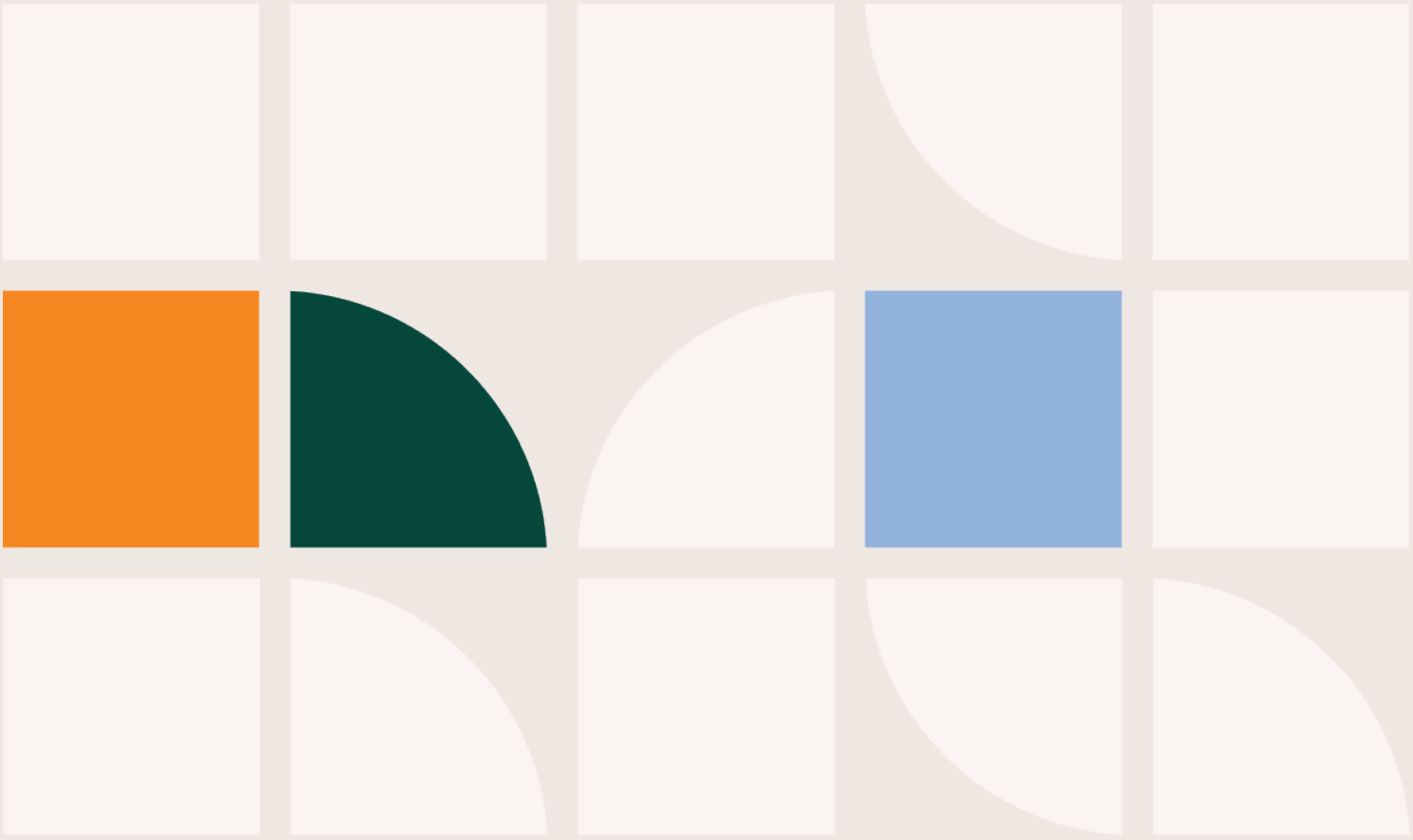
Woodville Litigation Funding

Disaster Recovery Plan

& Business Continuity Plan



PART 1 | INTRODUCTION

This document sets an executable plan in case of an emergency or disaster.

This document will be triggered in the event of:

- An epidemic, pandemic or disease
- A natural disaster
- A technology issue including but not limited to a data breach or cybersecurity attack
- A fire

This document consists of a Business Continuity element, which focuses on:

- Office Facilities
- Staff
- Safety

It also consists of a Disaster Recovery element, which focuses on

- IT recovery
- Back Up Facilities
- Telecoms Recovery

By incorporating both types of planning, this document seeks to address critical events and actions that impact staff, facilities and IT components in order to provide a holistic view of the recovery and continuity process.

In the following pages, you will find the various event types described and appropriate responses outlined.

PART 2 | GENERAL INFORMATION

Business Name:	Woodville Consultants Ltd
Address:	5 Gelliwasted Road, Pontypridd Rhondda Cynon Taf, Wales, CF37 2BP
Date:	22 August 2024
Prepared By:	David Palmer

PART 3 | MAINTAINING DOCUMENT & VERSION CONTROL

Document Control

The maintenance and updating of this document is the responsibility of:

DEPARTMENT / MEMBER	DATE APPROVED	SIGNATURE
IT Department	22 August 2024	D Palmer

Version Control

This section shows whenever the plan has been modified so that changed can be tracked and monitored:

VERSION	DATE	AMENDMENTS	DETAILS	AMENDED BY
1.0	22/08/2024	Initial Document	BCP & DR Plan	David Palmer

DRP Contacts

For further information regarding this document: please contact

	COMPANY	LANDLINE	EMAIL
David Palmer	Woodville Consultants	01443 561523	davidp@wclate.com

PART 4 | ACCESSING CURRENT RISKS

Business Continuity Plans (BCP's) and Disaster Recovery Plans (DRP's) are tools to assist the organisation in preparing for disaster occurrences that could make some or all the resources unavailable for a period of time.

Disasters come in varying forms. We group them as follows;

TYPE 1	File loss, partial system failure, phone system failure, internet failure
TYPE 2	Loss of location but the system is not affected (most pressing threat in UK at present)
TYPE 3	Full loss of system but the location is not affected e.g. Virus, equipment theft, hacking, or power outage
TYPE 4	Full loss of location and system
TYPE 5	Loss of staff (e.g. Wholesale headhunting, lotto syndicate, bird flu etc.)

PART 4.1 | RISK: LOSS OF KEY MEMBERS OF STAFF (TYPE 5)

Likelihood Unlikely

Impact Short-term disruption

In the event of this risk, the organisation will engage external recruitment consultants to source a replacement.

PART 4.2 | RISK: INABILITY TO ATTRACT NEW STAFF (TYPE 5)

Likelihood Unlikely

Impact Short-term disruption

In the event of this risk, the organisation can internally restructure its human resources to respond to an increased workload pending the recruitment of new staff.

PART 4.3 | RISK: INABILITY TO ACCESS SYSTEMS (TYPE 3)

Likelihood Unlikely

Impact Short-term disruption

In the event of this risk, the organisation will liaise with the IT support to solve the problem at the relevant third party service provider. The organisation enters into a service agreement with the 3rd party service providers and regularly reviews the service levels and support provided and take this into consideration when deciding to renew or replace the agreement.

PART 4.4 | RISK: LOSS OF DATA WITHIN SYSTEMS (TYPE 3)

Likelihood Unlikely

Impact Short-term disruption

In the event of this risk, the organisation will liaise with the IT support to solve the problem and recover data held on backup servers (managed by 3rd party provider). All data is regularly backed up into the cloud and can be rolled back if this issue occurs.

PART 4.5 | RISK: DATA BREACH (TYPE 3)

Likelihood Unlikely

Impact Short-term disruption

In the event of this risk, the organisation will liaise with its IT team and 3rd party service providers to source, identify and eliminate the breach and recover data from backup servers.

PART 4.6 | RISK: PHYSICAL DAMAGE TO HARDWARE (TYPE 1)

Likelihood Unlikely

Impact Short-term disruption

In the event of this risk, the organisation will replace the damaged hardware with spares or source new hardware on an ownership or lease basis. As all systems are cloud based, these can be accessed remotely from any device.

PART 4.7 | RISK: LOSS OF ACCESS TO BUSINESS PREMISES (TYPE 2)

Likelihood Unlikely

Impact Short-term disruption

In the event of this risk, the organisation will liaise with internal staff members to relocate to another site or work remotely. As all systems are cloud based, these can be accessed remotely from any device.

PART 4.8 | RISK: VANDALISM OR ACTS OF GODS (TYPE 1)

Likelihood Unlikely

Impact Short-term disruption

In the event of this risk, the organisation will replace any damaged hardware with spares or source new hardware on an ownership or lease basis and notify staff to work remotely. As all systems are cloud based, these can be accessed remotely from any device

PART 5 | OUTSOURCED SERVICE PROVIDER(S)

We have reviewed the risks pertaining to services or operational functions where the organisation outsources to a 3rd party service provider.

PART 5.1 | RISK: LOSS OF SERVICE (TYPE 3)

Likelihood Unlikely

Impact Short-term disruption

In the event of this risk, the organisation will liaise with the service provider to resolve the issue, if this cannot be resolved. The organisation will conduct the outsourced operations in-house or source another outsourcing service provider.

PART 5.2 | RISK: UNEXPECTED TERMINATION OF AGREEMENT/SERVICE (TYPE 3)

Likelihood Unlikely

Impact Short-term disruption

In the event of this risk, the organisation will liaise with the service provider to resolve the issue, if this cannot be resolved. The organisation will conduct the outsourced operations in-house or source another outsourcing service provider.

PART 6| RECOVERY PRIORITIES

In the event of any of the above mentioned risks, the organisations recovery priorities will be as follows;

- Secure the health and safety of it's staff
- Communicate to our customers (individually or on a public platform) of a disruption to the continuity of our operations
- Seek to remedy the disruption and restore service continuity

PART 7.1| IN THE EVENT OF A DISASTER

In the event of a disaster, below is a table listing the parties who will be contacted, in this order, in any emergency or disaster that disrupts business operations.

DEPARTMENT / ROLE	CONTACT NAME
Directors	Ann Marie Bell & Peter Legge
Head of IT	David Palmer
Operations Manager	Mark Palmer
Head of Data Analysis	Angharad Price

Once the disaster recovery team has been notified of the event, we then contact any external parties that are required to be notified of the disruption to business operations.

PART 7.2| TIMELINES IN EVENTS OF DISASTER EVENT

In the event of a disaster, below is a table listing the parties who will be contacted, in this order, in any emergency or disaster that disrupts business operations.

Type 1 File Loss, system failure, phone system failure, internet failure, hardware failure.

Action: Contact IT Support Provider
Response / Recovery Time: Determined by system Provider

Type 2 Loss of Location but the system is not affected

Action: Relocate Staff to home or second location
Response / Recovery Time: Within 24 Hours

Type 3 Loss of systems but the location is not affected

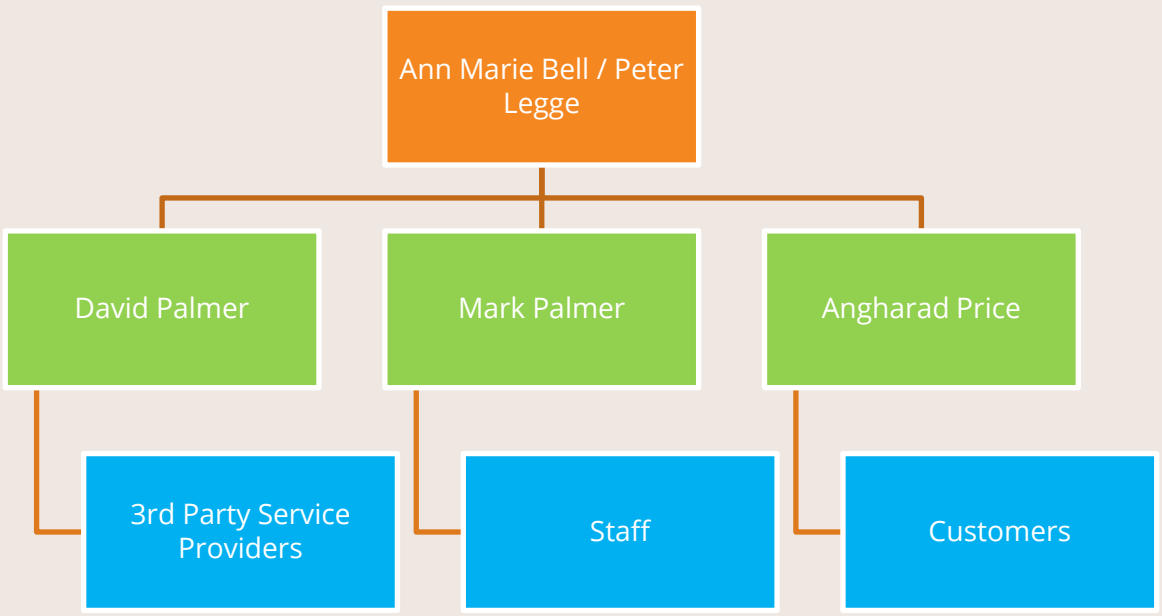
Action: Contact IT Support Provider
Response / Recovery Time: Determined by system Provider

Type 4 Full lose of site and system

Action: Relocate Staff, Contact IT Support Provider
Response / Recovery Time: Determined by system Provider

PART 7.3| COMMUNICTING THE DISASTER EVENT

The most efficient way to contact all staff members is to have a "Communication Contact Tree". This enables one staff member to contact several other staff members, 3rd party service providers and customers to advise them of the disaster event.



PART 8| DISASTER RECOVERY PLAN REVIEW

The Company shall review this Plan every 12 months in order to ensure that it remains up-to-date and fit for purpose.

This Disaster Recovery Plan has been approved and authorised on behalf of Woodville Consultants Limited by:

Signature: Ann Marie Bell Date: 28th August 2024

Woodville Litigation Funding

5 Gelliwasted Road
Pontypridd, CF37 2BP
info@woodville-consultants.co.uk