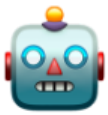

34. Disaster Recovery Plan and Business Continuity Policy

Reviewed By: Melissa Munnich

Review Date: 16th September

The purpose of this **Business Continuity and Disaster Recovery (BCDR) Policy** is to ensure that Woodhurst can effectively respond to, manage, and recover from any disruption to its business operations. The policy outlines the framework for maintaining essential functions during and after a disaster or significant interruption. It applies to all departments, employees, contractors, and critical partners.

This BCDR Policy integrates specific IT Disaster Recovery Plans and forms part of Woodhurst's commitment to operational resilience, ensuring our ability to continue critical services in the face of adverse events.

34.1 Objectives

The key objectives of this BCDR Policy are to:

- Achieve a **Recovery Time Objective (RTO)** of 4 hours and a **Recovery Point Objective (RPO)** of 30 minutes for critical services to ensure minimal downtime and data loss.
- Ensure the safety and well-being of employees, clients, and stakeholders during disruptions.
- Maintain continuity of critical business operations with minimal disruption.
- Protect and secure company assets, including data, infrastructure, and intellectual property.

- Provide a clear, structured response to disasters and significant business interruptions, ensuring rapid recovery.

34.2 Regulatory and Legal Compliance

Woodhurst is committed to complying with all relevant regulatory and legal requirements, including those issued by the **Financial Conduct Authority (FCA)**, the **Prudential Regulation Authority (PRA)**, and data protection laws such as the **General Data Protection Regulation (GDPR)**. The company also adheres to best practices for operational resilience in the financial services industry.

34.3 Roles and Responsibilities

- **Board of Directors, Head of IT, and Head of Operations**: Responsible for the overall BCDR strategy, aligning it with business objectives and regulatory compliance. They ensure that the policy is maintained, tested, and updated regularly.
- **Department Heads**: Accountable for identifying critical functions within their respective areas and ensuring that appropriate continuity and recovery procedures are in place.
- **Employees**: All employees are expected to be familiar with the BCDR policy, understand their roles during an interruption, and actively participate in training and drills to ensure preparedness.

34.4 Operational Resilience within Woodhurst

Woodhurst's operational resilience strategy underpins this BCDR policy. Key elements include:

- **Use of Cloud-Based Systems**: By leveraging cloud services such as **Microsoft Azure**, we ensure that data is accessible and backed up off-site, allowing rapid recovery in the event of an incident.
- **Regular Business Impact Analysis (BIA)**: Conducted annually, the BIA assesses the potential impact of disruptions, ensuring that critical functions are prioritised during recovery.

- **Redundancy and Failover Capabilities**: Critical systems are designed with redundancy to ensure seamless failover in the event of a service outage. Key dependencies include cloud service providers, secure backups, and internal IT personnel.

34.5 Business Continuity Plan (BCP)

The Business Continuity Plan (BCP) is designed to ensure that Woodhurst's critical business functions can continue during and after a disaster. The plan includes the following key components:

- **Recovery Time Objective (RTO) and Recovery Point Objective (RPO)**: Critical services are subject to an RTO of 4 hours and an RPO of 30 minutes, minimising operational downtime and data loss.
- **Identification of Key Dependencies**: We rely on cloud service providers (Microsoft Azure), internal IT personnel, and secure backups, which are reviewed regularly to ensure that they can support timely recovery.
- **Continuity Strategies**: These include remote working capabilities, alternative work sites, and resource reallocation to ensure that business operations continue without interruption.

34.5.1 Continuity of Critical Functions

Woodhurst has identified the key processes that must remain operational during a disruption, including client service delivery, data security, and communication systems. These are subject to the RTO and RPO targets, ensuring minimal disruption to operations.

34.5.2 Disaster Recovery Plan (DRP)

The Disaster Recovery Plan (DRP) outlines the steps and procedures to be followed to restore IT systems and data in the event of a disaster. The goal is to protect sensitive data, minimise downtime, and restore normal operations as quickly as possible.

34.5.2.1 Objectives

- Ensure the protection and recovery of critical IT systems and data.
- Minimise business disruption.
- Define clear roles and responsibilities for disaster recovery.
- Provide actionable steps for responding to different disaster scenarios (e.g., cyberattacks, hardware failure).

34.5.2.2 Scope

The DRP covers all critical IT infrastructure, including:

- Cloud services (**Microsoft 365, Azure, Slack, Notion, Pipedrive**).
- Endpoint devices (laptops, desktops, mobile devices).
- Network infrastructure (routers, firewalls, VPN).

34.5.2.3 Roles and Responsibilities

- **Disaster Recovery Lead (Josh Rix)**: Coordinates the disaster recovery process, communicates with stakeholders, and provides updates.
- **IT Support Team (Alex Bywater)**: Assists with technical recovery tasks, including data restoration and system monitoring.

34.5.2.4 Disaster Recovery Steps

1. **Risk Assessment**:

Regularly assess and update potential risks to IT infrastructure, including cyber threats and hardware failures.

2. **Backup and Recovery Procedures**:

Full backups are conducted weekly, with incremental backups occurring multiple times daily. Data recovery is prioritised for critical systems to minimise disruption.

3. **Communications Plan**:

A communication strategy is in place to notify all stakeholders (employees, clients, partners) during incidents, providing regular updates via email, phone, and messaging platforms.

4. **Systems Restoration**:

Hardware will be replaced or repaired, software reinstalled, and data restored from backups to the appropriate systems.

5. **Testing and Verification**:

All systems are rigorously tested after restoration to ensure proper functionality and accurate data recovery.

6. **Post-Recovery Review**:

After full restoration, a review of the recovery process will be conducted to identify gaps or improvements for future incidents.

34.6 Pandemic Response Strategy

Woodhurst recognises the potential operational disruption posed by pandemics and public health emergencies. To ensure resilience and service continuity, the following pandemic response measures are in place:

- Remote Working Infrastructure: All employees are equipped to work remotely using secure, cloud-based tools including Microsoft 365 and communication platforms such as Teams and Zoom. Our remote work setup allows seamless continuity of operations.
- Health and Safety Measures: In the event that in-person work is necessary, Woodhurst follows all applicable UK government and public health guidance to ensure the safety of employees and visitors.
- Communication Protocols: In the event of a pandemic-related disruption, regular updates will be provided to staff and clients to ensure transparency and alignment.
- Service Prioritisation: During prolonged workforce disruption, services will be triaged based on criticality, with clear prioritisation to maintain client deliverables.

The pandemic response strategy is reviewed alongside the Business Continuity Plan annually and updated based on lessons learned and evolving public health guidance.

34.7 Climate-Related Risks and Environmental Disruptions

Woodhurst acknowledges that climate change presents an evolving risk landscape, including physical risks such as extreme weather events and infrastructure disruptions.

As part of our risk management and continuity planning, we:

- Consider climate-related disruptions, including heatwaves, flooding, and severe weather, in our business impact assessments.
- Maintain the ability for staff to work remotely from alternate locations in the event of localised access issues due to weather.
- Operate with cloud-based systems hosted on Microsoft Azure, which maintains geographically diverse data centres with environmental resilience.
- Commit to reviewing physical site risks annually and incorporating climate resilience considerations in future infrastructure decisions.

These considerations are integrated into our continuity planning to ensure Woodhurst remains resilient to the long-term and acute impacts of climate change.

34.8 Maintenance of the BCDR Plan

- **Annual Review**: The BCDR and DRP will be reviewed and updated annually, or whenever significant changes occur in the IT infrastructure.

This Business Continuity and Disaster Recovery Policy ensures that Woodhurst maintains operational resilience, enabling critical business functions to continue with minimal disruption.