[Company Name & Logo]

**Business Continuity Plan**

|  |  |
| --- | --- |
| Version Control | |
| Version |  |
| Author Name |  |
| Date of Last Update |  |
| Approved by |  |

**Ensuring Operational Resilience and IT Recovery**

**Contents**

[1. Objectives of the Plan 3](#_Toc193792039)

[2. Roles and Responsibilities: Crisis Management Team (CMT) 3](#_Toc193792040)

[2.1 IT Recovery Team 3](#_Toc193792041)

[2.2 Business Recovery Team 3](#_Toc193792042)

[3. Business Impact Analysis 4](#_Toc193792043)

[4. Response Plan 4](#_Toc193792044)

[4.1 Unavailability of Site 5](#_Toc193792045)

[4.2 Unavailability of Systems 5](#_Toc193792046)

[4.3 Unavailability of People 6](#_Toc193792047)

[5. Business Continuity Procedures 6](#_Toc193792048)

[5.1 Fire or Physical Disaster 6](#_Toc193792049)

[5.2 Cybersecurity Breach 6](#_Toc193792050)

[5.3 Natural Disasters 6](#_Toc193792051)

[6. Related Policies 7](#_Toc193792052)

[7. Review and Maintenance 7](#_Toc193792053)

# 1. Objectives of the Plan

The objectives of this plan are to:

* Maintain the continuity of essential business processes.
* Minimize operational disruption in the event of an emergency.
* Establish a recovery framework to restore operations swiftly.
* Ensure the safety of all employees and the protection of critical assets.
* Fulfill legal and regulatory requirements for business continuity.

# 2. Roles and Responsibilities: Crisis Management Team (CMT)

## 2.1 IT Recovery Team

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Name | |  | | --- | |  |   Title | |  | | --- | |  |   Roles and Responsibilities | |  | | --- | |  |   Role In Plan |
| [Name] | IT Manager | Ensure IT systems are recovered as per the recovery plan | Plan Owner |
| [Name] | Database Analyst | Oversee data recovery processes | Data Specialist |
| [Name] | Server Support Technician | Manage server restoration and connectivity | Server Specialist |

## 

## 2.2 Business Recovery Team

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Title | Roles and Responsibilities | Role in Plan |
| [Name] | Business Manager | Coordinate non-IT related recovery efforts | Plan Owner |
| [Name] | HR Lead | Ensure employee communication and support | HR Specialist |
| [Name] | Finance Lead | Restore financial operations and systems | Finance Specialist |

## 3. Business Impact Analysis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Department/Function | Likelihood of Disruption | Business Impact | Risk Level | Mitigation Strategy |
| IT Infrastructure | Likely | High | Significant | Backup systems and off-site storage |
| Finance | Moderate | Major | Medium | Cloud-based accounting systems |
| Operations | Rare | Severe | Low | Redundant operations site available |

# 4. Response Plan

## 4.1 Unavailability of Site

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted Area | Action Plan | Responsible Role | Time to Execute |
| Office | Notify Crisis Management Team and activate the remote work plan | Business Continuity Manager | [Time] |
| Data Center | Switch to secondary data center | IT Manager | [Time] |
| Communications | Use alternative telecommunication systems | Comms Lead | [Time] |

## 4.2 Unavailability of Systems

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted System | Action Plan | Responsible Role | Recovery Time |
| Email Servers | Switch to backup email systems | IT Manager | [Time] |
| CRM System | Enable cloud-based backup system | CRM Administrator | [Time] |
| File Storage | Use offsite backups | IT Support Lead | [Time] |

## 4.3 Unavailability of People

|  |  |  |  |
| --- | --- | --- | --- |
| Key Role | Interim Arrangement | Responsible for Activation | Recovery Time |
| IT Manager | Delegate responsibilities to IT Support Lead | Head of Operations | [Time] |
| Finance Lead | External accounting firm to step in temporarily | CFO | [Time] |
| HR Manager | HR Assistant to Manage Employee queries | Head of HR | [Time] |

# 5. Business Continuity Procedures

## 5.1 Fire or Physical Disaster

* Immediate evacuation of all employees following the fire safety protocol.
* Activation of offsite working arrangement within 2 hours.
* Restoration of critical IT services within 3 hours from the backup site.

## 5.2 Cybersecurity Breach

* Isolate affected systems to prevent further compromise.
* Notify IT and Cybersecurity teams immediately.
* Activate alternative communication methods while recovery is in progress.

## 5.3 Natural Disasters

* Assess damage to infrastructure and employee safety.
* Enable full-scale remote work as a contingency for an affected area.
* Notify clients of expected downtime and provide updates as recovery progresses.

# 6. Related Policies

* **Risk Management Policy:** Guides to decision-making on risk mitigation strategies.
* **Health and Safety Policy:** Ensures employee well-being during a crisis.
* **Information Security Policy:** Safeguards data in line with ISO standards.
* **Data Protection Policy:** Complies with legal obligations to protect personal data.

# 7. Review and Maintenance

* **Frequency of Review:** Annually, or after each activation of the plan.
* **Next Review Date:** [dd/mm/yyyy]
* **Document Owner:** [Document Owner's Name]  
  The document owner is responsible for ensuring the plan remains up to date and effective.
* **Plan Testing:** Full-scale testing is conducted bi-annually to ensure all parts of the plan are functional.