<Organization Name>

**Business Continuity Plan**

|  |  |
| --- | --- |
| **Standard** | ISO/IEC 27001:2022 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision History** | | | |
| **Version** | **Date** | **Revision Author** | **Summary of Changes** |
| <Version Number> | <DD/MM/YYYY> | <Author Name> | *Initial Version* |

|  |  |
| --- | --- |
| **Distribution List** | |
| **Name** | **Title** |
| <Name> | IT Manager |
| <Name> | CEO |
| <Name> | Business Continuity Lead |
| <Name> | <Title> |

|  |  |  |  |
| --- | --- | --- | --- |
| **Approval** | | | |
| **Name** | **Position** | **Signature** | **Date** |
| <Approver Name> | Chief Information Security Officer (CISO) | <Signature> | <DD/MM/YYYY> |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision History** | | | | |
| **Version** | **Date** | **Prepared By** | **Approved By** | **Changes/Notes** |
| <version No> | <DD/MM/YYYY> | <Name> | <Name> | *Initial Version* |

|  |  |  |
| --- | --- | --- |
| **Distribution List** | | |
| **Recipient Name** | **Department** | **Distribution Date** |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |
| <Name> | <Department> | <DD/MM/YYYY> |

**Table of Contents**

[Plan Purpose and Scope 1](#_Toc179796424)

[Plan Objectives 1](#_Toc179796425)

[Activation Criteria and Procedures 1](#_Toc179796426)

[Procedure for Activation 1](#_Toc179796427)

[Implementation Procedures 2](#_Toc179796428)

[Procedure Description 3](#_Toc179796429)

[Cloud-Based Systems 3](#_Toc179796430)

[On-Premise Services 3](#_Toc179796431)

[Infrastructure Services 3](#_Toc179796432)

[Roles, Responsibilities, and Authorities 4](#_Toc179796433)

[Communication Requirements and Procedures 5](#_Toc179796434)

[Means of Communication 5](#_Toc179796435)

[Internal Communication 6](#_Toc179796436)

[External Communication 7](#_Toc179796437)

[Additional Notes 8](#_Toc179796438)

[Operational Continuity Strategies 9](#_Toc179796439)

[Site Unavailability 9](#_Toc179796440)

[System Unavailability 10](#_Toc179796441)

[People Unavailability 11](#_Toc179796442)

[Additional Notes 12](#_Toc179796443)

[Internal and External Interdependencies and Interactions 13](#_Toc179796444)

[Resource Requirements 13](#_Toc179796445)

[Information Flow and Documentation Processes 13](#_Toc179796446)

[Restoration of Normal Service 13](#_Toc179796447)

# Plan Purpose and Scope

The purpose of this Business Continuity Plan (BCP) is to ensure the recovery and continuation of <Organization Name>'s IT systems and critical business operations following a major disruption. This plan covers disruptions caused by hardware failures, software issues, physical damage, or other incidents that impact critical IT systems.

# Plan Objectives

* Recover IT systems at an alternative location within the defined Response Time Objective (RTO).
* Ensure continuity of critical business operations in a limited capacity until full systems are restored.
* Protect sensitive data and ensure compliance with ISO 27001:2022 information security management controls.

# Activation Criteria and Procedures

This plan will be activated under the following scenarios

* A major incident that significantly affects IT systems.
* Localized incidents that require limited activation.

## Procedure for Activation

* The Incident Response Team (IRT) will notify the appropriate recovery team(s).
* Localized activation can be initiated by the Plan Owner or the CISO.

# Implementation Procedures

This section outlines the actions required to restore services.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Service** | **Server/System** | **Action Required** | **Person Responsible** | **Priority** |
| Cloud-Based Systems | CRM Server (SRV04) | Activate cloud instance and restore latest backup | IT Manager | High |
| <Name> |
| Accounts Server (SRV08) | Recover accounts server using cloud resources | Server Support | High |
| <Name> |
| File and Print Server (SRV01) | Set up cloud replication for file and print services | Network Analyst | Medium |
| <Name> |
| On-Premises Services | Phone System | Reconfigure phone services and reroute to backup system | Telecom Specialist | Medium |
| <Name> |
| Asset Management System | Restore local backup of asset management system | Application Specialist | High |
| <Name> |
| Time Tracking System | Set up time tracking system on alternate local server | HR System Admin | Low |
| <Name> |
| Data Query Tools | Restore data query services using alternate local database instance | Database Analyst | Medium |
| <Name> |
| Infrastructure Services | Network Access | Set up alternate VPN for remote employees to access IT services | Network Specialist | High |
| <Name> |
| Internet Access | Restore primary internet connection or enable backup ISP | IT Manager | High |
| <Name> |
| Power Systems | Activate uninterruptible power supply (UPS) and test generator backup | Facility Manager | Critical |
| <Name> |

*NOTE: Please add any additional services that are relevant to the organization to this table and remove any services that do not apply to your specific environment.*

## Procedure Description

### Cloud-Based Systems

* **CRM Server (SRV04) –** The CRM system will be restored from the cloud with minimal downtime using backups stored in AWS.
* **Accounts Server (SRV08)** **–** The accounts server will be reactivated in the cloud with backup data to ensure financial operations continue.
* **File and Print Server (SRV01)** **–** The file and print services will be restored using cloud infrastructure to maintain essential business operations.

### On-Premise Services

* **Phone System** **–** The phone system will be rerouted to a secondary local system or an alternate VoIP service to maintain internal and external communications.
* **Asset Management System** **–** The asset management system will be restored from a local backup, enabling the company to track and manage resources.
* **Time Tracking System** **–** An alternative local server will be used to restore the time tracking system, ensuring employee work hours are captured.
* **Data Query Tools** **–** Restore data query tools using an alternate database instance to allow business teams to access critical data for operations.

### Infrastructure Services

* **Network Access** **–** A virtual private network (VPN) will be set up to provide remote access to key services for employees working from home or remote sites.
* **Internet Access** **–** If the primary internet connection is disrupted, a backup ISP or alternate connection will be activated.
* **Power Systems** **–** The uninterruptible power supply (UPS) will be checked, and the backup generator will be tested to ensure continuity during any power disruptions.

# Roles, Responsibilities, and Authorities

|  |  |  |
| --- | --- | --- |
| **Name** | **Title** | **Role** |
| <Name> | IT Manager | Plan Owner |
| <Name> | Server Support Technician | Server Specialist |
| <Name> | Network Analyst | Network Specialist |
| <Name> | <Title> | <Role> |
| <Name> | <Title> | <Role> |

# Communication Requirements and Procedures

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Means of Communication | | | | |
| **Method** | **Purpose** | **Responsible Party** | **Frequency** | **Additional Notes** |
| Telephone (Landline) | Primary communication method for real-time updates | IT Manager / IRT Lead | As needed during the incident | Ensure contact list is up to date |
| <Name> |
| Mobile Phone | Backup method if landlines are unavailable | IRT Members / Key Personnel | As needed | Phones should be fully charged and easily accessible |
| <Name> |
| Microsoft Teams (Collaboration Tool) | Provide updates and collaboration for remote teams | IRT Lead | Regular intervals | Use Teams for documentation and shared communication logs |
| <Name> |
| Email | For non-urgent communication or follow-ups | IT Manager | Daily (if applicable) | Use encrypted email for sensitive information |
| <Name> |
| Two-Way Radio (if applicable) | Emergency communication in case of phone outage | Facility Manager | During physical disruptions | Ensure radios are charged and tested regularly |
| <Name> |
| <Method> | <Purpose> | <Title> | <Frequency> | <Additional Notes> |
| <Name> |

*NOTE: This table can be updated to reflect any changes in the organization's structure, communication methods, or designated personnel to ensure it remains aligned with the current communication protocols and responsibilities.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Internal Communication | | | | | | |
| **Type** | **Stakeholders** | **Method** | **Purpose** | **Responsible Party** | **Frequency** | **Additional Notes** |
| IRT Updates | IRT Members, Senior Management | Telephone / Teams / Mobile Phone | Real-time updates on incident handling | IRT Lead | Hourly or as needed | Ensure key contacts are available |
| <Name> |
| Employee Notifications | All Employees | Email / Teams | Notify employees about the incident status | HR / Communication Lead | Regular intervals (e.g., every 2 hours) | Pre-drafted email templates for incident notification |
| <Name> |
| Critical Department Heads | IT, HR, Finance, Operations | Telephone / Teams / Mobile Phone | Provide department-specific updates | IRT Lead | Hourly or as needed | Prioritize communication with departments critical to recovery |
| <Name> |
| <Type> | <Stakeholders> | <Method> | <Purpose> | <Responsible Party> | <Frequency> | <Additional Notes> |
| <Name> |

*NOTE: This table can be updated to reflect any changes in the organization's structure, communication methods, or designated personnel to ensure it remains aligned with the current communication protocols and responsibilities.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| External Communication | | | | | | |
| **Type** | **External Parties** | **Method** | **Purpose** | **Responsible Party** | **Frequency** | **Additional Notes** |
| Media | Media Outlets | Phone / Email | Coordinate public communications | Communication Lead | As needed | All media requests handled by IRT-approved personnel only |
| <Name> |
| Emergency Services | Police, Fire, Ambulance | Telephone / Radio | Coordinate emergency response | Security Manager | As needed | Pre-approve contact details and establish points of contact |
| <Name> |
| Disaster Recovery Provider | External DR Provider | Telephone / Teams | Activate disaster recovery services | IT Manager | As needed | Ensure DR contracts and SLAs are accessible |
| <Name> |
| Regulatory Authorities | Data Protection Authorities | Email / Telephone | Report any data breaches or regulatory issues | Compliance Manager | As needed (within legal timeframe) | Ensure all reports are compliant with legal requirements |
| <Name> |
| <Type> | <Stakeholders> | <Method> | <Purpose> | <Title> | <Frequency> | <Additional Notes> |
| <Name> |

*NOTE: This table can be updated to reflect any changes in the organization's structure, communication methods, or designated personnel to ensure it remains aligned with the current communication protocols and responsibilities.*

## Additional Notes

**Backup Communication Methods**

All personnel should have access to at least two forms of communication in case primary methods fail (e.g., mobile phones and two-way radios).

**Documentation**

All communications must be logged for post-incident review, and regular intervals should be set for status updates during the incident.

**Escalation Protocol**

If communication methods fail, escalate the issue to higher management for alternate arrangements.

# Operational Continuity Strategies

## Site Unavailability

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Minimum Requirement** | **Status During Disaster Scenario** | | **Recovery Steps** | **Responsibility** | **Time Taken** |
| Site Accessibility | Yes/No/Maybe | <Reason> | <Steps> | Business Continuity Manager | <Time in minutes> |
| <Name> |
| Critical Infrastructure | Yes/No/Maybe | <Reason> | <Steps> | CMT Leader | <Time in minutes> |
| <Name> |
| Safety of Personnel | Yes/No/Maybe | <Reason> | <Steps> | Facility Manager | <Time in minutes> |
| <Name> |
| Power Availability | Yes/No/Maybe | <Reason> | <Steps> | Facility Manager | <Time in minutes> |
| <Name> |
| Communication Availability | Yes/No/Maybe | <Reason> | <Steps> | IT Manager | <Time in minutes> |
| <Name> |
| Documents & Records | Yes/No/Maybe | <Reason> | <Steps> | IT Team | <Time in minutes> |
| <Name> |
| <Requirement> | Yes/No/Maybe | <Reason> | <Steps> | <Title/ Department> | <Time in minutes> |
| <Name> |

*The requirements and recovery steps outlined in this table can be added to or updated based on the organization's specific structure and operational needs.*

## System Unavailability

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Minimum Requirement** | **Status During Disaster Scenario** | | **Recovery Steps** | **Responsibility** | **Time Taken** |
| IT Systems Functionality | Yes/No/Maybe | <Reason> | <Steps> | IT Manager | <Time in minutes> |
| <Name> |
| Cloud Systems Availability | Yes/No/Maybe | <Reason> | <Steps> | IT Manager | <Time in minutes> |
| <Name> |
| On-Premise Systems | Yes/No/Maybe | <Reason> | <Steps> | IT Support | <Time in minutes> |
| <Name> |
| Internet Connectivity | Yes/No/Maybe | <Reason> | <Steps> | IT Team | <Time in minutes> |
| <Name> |
| Network Security | Yes/No/Maybe | <Reason> | <Steps> | Security Team | <Time in minutes> |
| <Name> |
| <Requirement> | Yes/No/Maybe | <Reason> | <Steps> | <Title/ Department> | <Time in minutes> |
| <Name> |

*The requirements and recovery steps outlined in this table can be added to or updated based on the organization's specific structure and operational needs.*

## People Unavailability

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Minimum Requirement** | **Status During Disaster Scenario** | | **Recovery Steps** | **Responsibility** | **Time Taken** |
| Personnel Availability | Yes/No/Maybe | <Reason> | <Steps> | HR Department | <Time in minutes> |
| <Name> |
| Remote Working Capability | Yes/No/Maybe | <Reason> | <Steps> | IT Manager | <Time in minutes> |
| <Name> |
| Alternate Personnel | Yes/No/Maybe | <Reason> | <Steps> | HR Department | <Time in minutes> |
| <Name> |
| Communication Systems | Yes/No/Maybe | <Reason> | <Steps> | Business Continuity Manager | <Time in minutes> |
| <Name> |
| Human Resource Support | Yes/No/Maybe | <Reason> | <Steps> | HR Manager | <Time in minutes> |
| <Name> |
| <Requirement> | Yes/No/Maybe | <Reason> | <Steps> | <Title> | <Time in minutes> |
| <Name> |

## Additional Notes

**Priority Tasks**

High-priority tasks should be performed first (e.g., establishing communication channels and recovering critical systems).

**Testing**

All procedures should be tested periodically to ensure readiness.

**Personnel Allocation**

Ensure that backup personnel lists are updated regularly to accommodate unavailability scenarios.

**Critical Systems**

Ensure that backup and cloud systems are periodically updated and accessible remotely.

# Internal and External Interdependencies and Interactions

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Ref** | **Plan Title** | **Plan Description** | **Plan Owner** |
| Plan001 | *Loss of Access to Building A* | *Move business activities to alternate site* | <Name> |
| Plan002 |  |  |  |

# Resource Requirements

|  |  |  |  |
| --- | --- | --- | --- |
| **Resource** | **Quantity** | **Source** | **Comments** |
| *Virtual Private Cloud* | *1* | *AWS via DR Supplier* | <Comment> |
| <Resource> |  |  |  |

# Information Flow and Documentation Processes

During incidents, all critical information must flow seamlessly between response teams to ensure proper documentation of actions and progress. Updates should be provided regularly to key stakeholders.

# Restoration of Normal Service

Once the IT systems are restored at the alternate location, top management will determine when to return to the primary location based on the extent of the damage and the availability of infrastructure.

**Appendix A: Contact Details of Key Personnel**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Role** | **Office Telephone** | **Mobile** | **Email** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Appendix B: Recovery Checklists**

|  |  |  |
| --- | --- | --- |
| **Task** | **Completion Date** | **Person Responsible** |
| *Confirm with Incident Response Team (IRT) about service availability* | <DD/MM/YYYY> | <Title> |
| <Name> |
|  |  |  |
|  |  |  |