

Business Continuity Policy

**Document Statistics**

|  |  |
| --- | --- |
| **Type Of Information** | **Document Data** |
| Document Title | Policy for Business Continuity |
| Document Code | PO/BCPPO/V03 |
| Date of Release | 11-Apr-2024 |
| Document Revision No | 3rd release of document |
| Document Owner | IT Executive |
| Documents Author(s) | IT Head |
| Document Change Reviewer | IT Head |
| Security Classification | Confidential |
| Document Status | Approved |

**Document approvers**

|  |  |  |
| --- | --- | --- |
| **Sr. No** | **Approver** | **Approver Contact(Email)** |
| 1 | Vice President Strategy & BIS | Rashmin Vyawahare <r.vyawahare@cloudextel.com> |

**Document Change Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Revision Date** | **Nature of Change** | **Date Approved** |
| 1 | 29th July 2022 | Initial Release | 28th July 2022 |
| 2 | 25th Dec 2023 | Revised Release | 27th Dec 2023 |
| 3 | 11th Apr 2024 | Revised Release | 11th Apr 2024 |

**Document Contact Point**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr. No.** | **Document/Process** | **Document Author** | **Document Primary Focal Point** |
| 1 | Business Continuity Policy | IT Head | IT Policy Folder |

**Document Reference List**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr. No** | **Reference No.** | **Document Name** | **Effective date** |
| 1 | PO/BCPPO/V01 | Business Continuity Policy\_Ver.1 | 28th July 2022 |
| 2 | PO/BCPPO/V02 | Business Continuity Policy\_Ver.2 | 27th Dec 2023 |

**Index**

Table of Contents

[1. Purpose and Scope 5](#_Toc165474471)

[1.1. Identification of Critical Systems: 5](#_Toc165474472)

[1.2. Business Functions Supported: 5](#_Toc165474473)

[1.3. Minimization of Disruption: 5](#_Toc165474474)

[2. Abbreviations and definitions 6](#_Toc165474475)

[3. Guidelines 6](#_Toc165474476)

[4. Background 6](#_Toc165474477)

[5. Business Continuity Management (BCM) Lifecycle 7](#_Toc165474478)

[5.1. Assessment Phase 7](#_Toc165474479)

[5.2. Planning Phase 7](#_Toc165474480)

[5.3. Testing Phase 8](#_Toc165474481)

[5.4. System Capacity and Demand 8](#_Toc165474482)

[5.5. Backup Strategy 9](#_Toc165474483)

[5.6. Office 365 Features 9](#_Toc165474484)

[5.7. Cloud PC Management Service 9](#_Toc165474485)

[5.8. Testing Business Continuity and Disaster Recovery Plans 10](#_Toc165474486)

[5.9. Policy Review 10](#_Toc165474487)

[5.10. Policy Approval 10](#_Toc165474488)

[5.11. Effective Date 10](#_Toc165474489)

[5.12. References 10](#_Toc165474490)

[6. Business Impact Assessment 10](#_Toc165474491)

[6.1. Essential Availability 10](#_Toc165474492)

[7. Supporting Policies and Standards 11](#_Toc165474493)

[8. Roles and Responsibilities 12](#_Toc165474494)

[9. Measurements 13](#_Toc165474495)

## Purpose and Scope

The purpose of the Business continuity plan is to explain the procedure being followed to maintain the confidentiality, integrity, and the availability of the business data at all the times by ensuring the continuity of critical business operations and minimize the impact of disruptions or disasters on our organization's ERPNext system hosted on **AWS** and **Microsoft Office 365** for emails. This policy establishes guidelines and procedures for business continuity planning, disaster recovery, and regular testing.

## Identification of Critical Systems:

CloudExtel recognizes ERPNext and Office365 as critical systems essential for the continuity of business operations.

## Business Functions Supported:

* + 1. **ERPNext:** This system supports vital functions including financial accounting, inventory management, order processing, and procurement and payments.
    2. **Office365:** Integral to internal communication, document storage, and collaboration among CloudExtel teams.

## Minimization of Disruption:

The primary objective of our Business Continuity Plan is to minimize disruption to critical systems such as ERPNext and Office365.

Strategies will be implemented to ensure the continuous operation of these systems during unforeseen events, including but not limited to backup procedures, redundancy measures, and proactive monitoring.

Business continuity plan has to be designed to prepare Excel Telesonic to cope with the effects of an emergency or crisis. It is intended that this document will provide the basis for a relatively quick and painless return to “business as usual” regardless of the cause.

This policy is applicable to all Temporary Staff, Employees and Process Owners working with Excel Telesonic India Pvt Ltd. All are expected to be familiar with and comply with this policy.

## Abbreviations and definitions

|  |  |  |
| --- | --- | --- |
| **Sr. No** | **Abbreviation/Definition** | **Explanation** |
| 1 | IS | Information systems |
| 2 | ISM | Information Security Manager |
| 3 | ISSC | Information Security Steering Committee |
| 4 | BCP | Business continuity Policy |
| 4 | DR | Disaster Recovery Policy |

## Guidelines

1. Define scope and responsibilities.
2. Perform risk and impact analysis.
3. Set acceptable downtime guidelines.
4. Test and update the plan regularly.
5. Implement security measures.
6. Ensure compliance with regulations.
7. Define remedies for non-compliance.

## Background

Excel Telesonic India Pvt Ltd. is using technology to deliver best possible services to its customers. However, this dependence also implies that any disruption in the business infrastructure may seriously hamper the ability to conduct normal business. This is especially true in the case of disasters, both natural and man-made.

The management of Excel Telesonic India Pvt Ltd has decided to formulate a Business Continuity Plan (‘BCP’) for the organization’s information technology systems and other systems, which are critical for the everyday functioning of the organization. A good business continuity plan has to do more than outline how Organizations data is backed up and restored. The plan must detail a specific set of procedures to follow in the case of an emergency.

Our organization is committed to maintaining the continuity of critical business operations and minimizing the impact of disruptions or disasters. We will achieve this by implementing a comprehensive business continuity plan and disaster recovery strategy that includes regular testing and updating of plans.

## Business Continuity Management (BCM) Lifecycle

## Assessment Phase

Conduct an assessment to identify critical business processes and objectives for inclusion in the business continuity program.

Perform a Business Impact Analysis (BIA) during the assessment phase to determine the potential impact of disruptions or disasters on critical business operations.

**Frequency of BIAs:**

* BIAs will be conducted annually to assess the potential impact of disruptions on CloudExtel's operations.
* Additionally, BIAs will be triggered by significant business changes such as mergers, acquisitions, infrastructure updates, or regulatory changes.

**Conditions Calling for a BIA:**

* A BIA will be initiated under the following circumstances:
* Annually as part of routine assessment procedures.
* Following significant business changes that could impact operations.
* In response to emerging threats or vulnerabilities identified through risk assessments.

## Planning Phase

Develop and implement resilience and recovery strategies during the planning phase.

Identify and document recovery procedures for critical business processes and systems.

Establish a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical business operations.

**Guidelines for Determining RTO and RPO:**

* RTO should be determined based on the actual time required to recover critical business functionality following a disruption. It should be less than the maximum allowable outage period determined appropriate by CloudExtel.
* RPO defines the maximum acceptable period during which data may be lost. It should be determined based on the criticality of data and the impact of potential data loss on business operations.

**Alignment with CloudExtel's Standards:**

* RTO and RPO should align with CloudExtel's standards for maximum allowable outage and data loss, respectively.
* These standards will be established in accordance with the criticality of business functions and data, ensuring that recovery objectives are in line with business continuity goals.

## Testing Phase

Test business continuity plans annually and update them as needed.

Test the disaster recovery plan to ensure an **RTO of 4 hours**.

Review After Action reports to validate test results and update plans accordingly.

**Clarity on RTO Determination:**

The RTO of 4 hours specified in the policy applies to ERPNext. It was determined based on factors such as business impact, SLAs, risk assessment, data criticality, recovery complexity, cost-benefit analysis, and stakeholder input.

It's important to note that RTOs can vary based on different capabilities or services within CloudExtel's technology stack and dependent systems. Therefore, detailed RTOs should be documented within the actual Business Continuity Plan for each critical capability or service.

**Documentation and Testing Procedures:**

During testing, it is essential to document the scope of the test, including the specific capability or service being tested, scenarios simulated, and outcomes observed.

Testing may involve planned tests of potential failure scenarios, where various disruptions are intentionally induced to evaluate the response and recovery procedures outlined in the BCP.

Results of testing should be thoroughly documented, including any issues identified, lessons learned, and recommendations for improvement.

## System Capacity and Demand

Ensure system capacity meets demand through regular capacity planning.

Utilize hardware, network, and datacenter redundancy for high availability and reliability during incidents.

## Backup Strategy

**Comprehensive Backup Strategy:**

The backup strategy outlined in the policy extends to encompass the entire business, ensuring that critical systems and data are adequately protected against potential disruptions.

Justification for the selection of systems to be backed up is based on the criticality of operations, data sensitivity, and regulatory requirements.

**Frequency and Scope of Backup Testing:**

* Backup testing is conducted regularly to validate the integrity and effectiveness of backup procedures.
* Testing occurs quarterly to ensure that backups are up-to-date and recoverable. Automatic backup occurs every 6 hours for our production ERPNext system and weekly backups are stored on additional server to address any larger disruption, like a full zone or region outage.
* Testing involves both partial and whole system backups, covering key components and data repositories critical to business operations.
* The scope of backup testing encompasses various scenarios to evaluate the resilience of backup systems and procedures under different conditions, including partial and complete data loss scenarios.

The only system owned by CloudExtel is ERPNext. The backup of Office-365 is managed by Microsoft as per the agreement.

## Office 365 Features

In leveraging Microsoft office 365, it is imperative that CloudExtel actively utilizes the features provided to enhance its business continuity posture. These features should not only be acknowledged but incorporated into daily operations to maximize their effectiveness in safeguarding critical business functions and data integrity. By actively utilizing the features offered by Microsoft Office 365, CloudExtel reinforces its resilience against potential disruptions and ensures seamless continuity of operations during adverse events.

## Cloud PC Management Service

Utilize the Cloud PC management service with regionally redundant architecture for high availability and a target uptime of 99.99%.

Ensure a Recovery Time Objective (RTO) of less than 4 hours and a Recovery Point Objective (RPO) of less than 30 minutes for changes made in the management service.

## Testing Business Continuity and Disaster Recovery Plans

Test business continuity plans at least annually per policies.

Validate resilience and recovery strategies against various potential incidents based on service criticality.

Review After Action reports to validate test results and update plans accordingly.

## Policy Review

This policy will be reviewed and updated annually or as needed to ensure alignment with organizational and technological changes.

## Policy Approval

This policy is approved by the CloudExtel Executive Team.

## Effective Date

This policy is effective as per the date mentioned in document matrix above.

## References

AWS Business Continuity Planning:

[Business Continuity Plan (BCP) - Disaster Recovery of Workloads on AWS: Recovery in the Cloud (amazon.com)](https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/business-continuity-plan-bcp.html)

Windows 365 Business Continuity and Disaster Recovery:

[Business continuity and disaster recovery with Windows 365 | Microsoft Learn](https://learn.microsoft.com/en-us/windows-365/business-continuity-disaster-recovery)

## Business Impact Assessment

A Business Impact Analysis (BIA) is the process by which a business unit management team identifies the functions most critical to meeting their service objectives. It is a facilitated process in which senior business unit management was interviewed and a report based on the findings and works with the business unit to develop plans and mitigation strategies.

## Essential Availability

The DR sites should replicate corporate office essential technological environment. It necessarily shall involve:

* + - There should be availability of Internet link to access all internet and intranet base application and for accessing the servers.
    - Server replicating entire current database.
    - Availability Common storage (critical Data /User Data /Departmental Data)
    - The critical servers should be accessible across the Excel Telesonic India network for accessing the required data as per the process.
    - Availability Mail server to work on Mail to communicate with Clients.
    - Workstation should be available as per requirement.
    - UPS and Inverters at the DR Sites ensuring smooth supply of power to run Servers, laptops and PCs for maximum time.
    - All employees should be able to access the mails through mail server or web mail.
    - The integrity check of Databases/ Mails/ Common storage will be done on weekly basis and logs are maintained as per the Backup Policy.
    - The Servers hosted at the DR-Site can be accessed via internet connectivity which is installed at both the DR-Site and with the secured access in case of Disaster.

## Supporting Policies and Standards

In conjunction with this Business Continuity Plan, CloudExtel recognizes the importance of aligning with other relevant policies and standards to ensure comprehensive preparedness for disruptions. Key supporting policies and standards that should be used together with the Business Continuity Plan include:

**Security Incident Management Policy:** Outlines procedures for detecting, reporting, and responding to incidents that could potentially impact business operations. Incident management procedures complement the Business Continuity Plan by providing a framework for immediate response and escalation during disruptive events.

**Access Management Policy:** Defines protocols for managing user access to systems, applications, and data within CloudExtel's infrastructure. Access management policies ensure that only authorized individuals have appropriate access privileges, thereby reducing the risk of unauthorized access or breaches that could disrupt business operations.

**Change Management Policy:** Establishes procedures for planning, implementing, and reviewing changes to IT systems and infrastructure. Change management policies ensure that changes are assessed for potential impacts on business continuity and are implemented in a controlled manner to minimize disruptions and maintain system integrity.

## Roles and Responsibilities

CloudExtel assigns specific roles and responsibilities to key personnel to ensure effective implementation and maintenance of the Business Continuity Plan. The following roles and their responsibilities are outlined:

**Chief Technology Officer (CTO):**

* Oversees the development and implementation of the Business Continuity Plan.
* Ensures alignment of the plan with organizational objectives and industry best practices.
* Provides strategic guidance on technology-related aspects of business continuity.

**Chief Information Officer (CIO):**

* Collaborates with the CTO to ensure that IT systems and infrastructure support the objectives of the Business Continuity Plan.
* Reviews and approves the overall strategy and objectives of the plan.
* Oversees the allocation of resources necessary for plan implementation and maintenance.

**Product Owner:**

* Collaborates with relevant stakeholders to identify and prioritize critical business functions and dependencies.
* Participates in Business Impact Analysis (BIA) to assess the potential impact of disruptions on business operations.
* Works with the BCP team to ensure that the plan addresses the continuity needs of key products and services.

**Business Continuity Manager:**

* Leads the development, implementation, and maintenance of the Business Continuity Plan.
* Coordinates BIA activities, including the identification of critical systems, functions, and resources.
* Facilitates plan testing, exercises, and training to ensure preparedness for disruptions.
* Oversees all aspects of business continuity planning, including the calculation of Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

## Measurements

CloudExtel leverages specific features within Microsoft 365 to fortify its business continuity capabilities. The adoption of these features is integral to minimizing disruptions and ensuring the seamless operation of critical business functions.

**Contribution to Business Continuity:**

The utilization of features such as **Azure Information Protection**, **Azure Active Directory**, etc directly contributes to CloudExtel's resilience against potential disruptions by facilitating remote collaboration, data accessibility, and seamless communication during adverse events.

**Alignment with RTO and RPO:**

These features have been strategically integrated into CloudExtel's Business Continuity Plan to align with Recovery Time Objective (RTO) and Recovery Point Objective (RPO) calculations. By leveraging Microsoft 365 capabilities, CloudExtel enhances its ability to meet RTOs by expediting the recovery of essential functions and reduces RPOs by ensuring timely data restoration.

By prioritizing the utilization of Microsoft 365 features tailored to CloudExtel's business continuity needs, the organization strengthens its resilience and ensures operational continuity in the face of disruptions.