**Business Continuity Plan**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_nabz1upydlws) **3**

[**Scope**](#_eynls6nonuku) **4**

[**Business Continuity Plan**](#_zcme8zt6jk2a) **4**

[**Business Continuity Committee**](#_ajtznqio2twg) **5**

[**Recovery Time Objective (RTO)**](#_r0lluf4zqrgg) **5**

[**Communication channels**](#_13beguq0whh9) **5**

[**Business Continuity Testing**](#_bjz23dqyqauk) **6**

[**Change, Review, and Update**](#_w1o88vxspwq8) **6**

[**Disciplinary Action**](#_qvp6mc55r7d6) **6**

[**Responsibility**](#_d61m2z8uqfoy) **6**

[**Related Documents**](#_vfgiehxqofzj) **6**

# **Purpose**

This plan is created to recognize threats and risks facing the company and provide procedures that ensure personnel and assets are protected and function in a disaster.

# **Scope**

The scope of this plan is focused on localized disasters such as fires, floods, and other localized natural or man-made disasters. This plan is not intended to cover major regional or national disasters. The scope of this plan covers internal and external issues, interested parties, their needs and expectations, legal and regulatory compliance obligations.

This plan is separate from our Disaster Recovery Plan, which focuses on recovering technology facilities and platforms.

# Business Continuity Plan

* Business Impact Assessments (BIAs) need to be conducted upon onboarding new, business-critical vendors.
* IT Manager with Head of Finance and Legal Counsel should identify the key events that can disrupt their processes and their potential adverse impact, financial & non-financial.
* The scope of the Business Continuity Plan should take into account relevant factors, including customer requirements, legal regulations, and industry requirements.
* The following should be considered while implementing any Business Continuity Plan:
  + Identify critical business functions, applications, and supporting technologies.
  + Develop an appropriate, cost-effective recovery strategy.
  + Identify backup locations with the necessary infrastructure to support the recovery needs.
  + Identify the management and membership of the disaster response and recovery teams.
  + Identify and document the required recovery actions, identify and ensure the availability of required resources, and compile this information as the recovery plan
  + Train the recovery teams in the performance of their specific tasks.
  + Identify functional team, recovery support, and response capabilities.
  + Develop an ongoing testing and maintenance program to ensure that all processes of the IT department are in a constant state of recovery readiness.
* All critical resources should be logically classified by recovery priority.

## **Business Continuity Committee**

The Top Management Team and IT Security Team are responsible for promoting the development and implementation of the Business Continuity Plan, establishing and coordinating business continuity activities while ensuring the enforcement, dissemination, and annual revision of this Policy.

| **Name** | **Role** | **Contact** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## **Recovery Time Objective (RTO)**

* The Recovery Time Objective is the maximum tolerable length of time when the service can be down. It depends on the criticality of the systems involved, SLA with a cloud provider, and SLA with our clients, and is *[n]* hours.
* In the case of service unavailability during non-business hours, the Recovery Time Objective can increase, and the recovery will be made during business hours the next day.

## **Communication channels**

For any crisis event, as described throughout this continuity plan, the following order of communication should be applied:

* Use Slack to inform all team members of the situation and advise on actions (#general, @channel to trigger notifications).
* Use Google email to duplicate communication messages.

## **Business Continuity Testing**

* The primary reason for testing and exercising the Business Continuity Plan is to simulate a more or less realistic situation to find out what does not work.
* *[Company]* performs testing of this Business Continuity Plan annually or more often in the case of any changes. The IT Manager is responsible for coordinating and conducting a rehearsal of this Business Continuity Plan.
* Business Continuity Committee prepares BCP Testing Program to determine if the activities would be recovered within the recovery time objective, whether all the employees know their roles, etc.
* Whenever the BC Plan is enacted, it must be followed up with a retrospective to identify lessons learned.
* The last thing done in the testing program is a review of results and comparing them with the objectives set before. Also, the IT Manager reports the results to the top management.

# **Change, Review, and Update**

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. Changes to this policy shall be exclusively performed by IT Manager.

# **Disciplinary Action**

Employees who violate this policy may face disciplinary consequences in proportion to their violation. *[Company]’s* management will determine how severe an employee’s offense is and take the appropriate action.

# **Responsibility**

The IT Manager is responsible for ensuring this policy is followed.

This policy shall be reviewed yearly or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related Documents**

* Disaster Recovery Plan
* Incident Response Plan