Business Continuity & Disaster Recovery Plan

Version: 1.0

Status: Formal Plan

1. Purpose

This document outlines business continuity (BC) and disaster recovery (DR) procedures for 2BrightSparks Pte. Ltd., ensuring ongoing software availability, support operations, and preservation of critical business functions in the event of disruption.

2. Scope

This plan applies to all 2BrightSparks' internal systems, infrastructure, and personnel. This includes:

- Internal systems supporting licensing, purchasing, website hosting, and customer support.
- Development infrastructure and source code repositories.
- Employee operational workflows and communication channels.

2.1. Customer Data Exclusion (Critical)

A core principle of 2BrightSparks' operation is that **customer-generated backup data created by SyncBack products is not stored by 2BrightSparks.** Customers control their own backup destinations and are responsible for their own data recovery.

This BC/DR plan exclusively covers 2BrightSparks' internal operational infrastructure and services.

3. Objectives

- Maintain critical business operations with minimal downtime.
- Ensure the integrity and recoverability of internal systems and data.
- Communicate promptly and clearly with internal teams, customers, and stakeholders.
- Restore critical services within the defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

4. Plan Activation & Declaration

4.1. Activation Triggers

This plan is immediately activated upon the confirmation of any of the following events:

- A critical business function (see section 7) is down for more than 60 minutes.
- A confirmed, significant security breach or data compromise.
- Total loss of the primary hosting environment or a critical cloud provider.
- Any event where key personnel determine that normal operations are not possible.

4.2. Declaration Authority

- **Primary Authority:** The **Incident Lead** has the primary authority to declare a disaster and activate this plan.
- **Secondary Authority:** In the absence of the Incident Lead, a member of **Management** will assume this authority.

5. Roles, Responsibilities & Contact Chain

The following team members are responsible for executing this plan.

Role	Responsibility	Primary Position	Backup Position	Emergency Contact Method
Incident Lead	Coordinates the entire response, makes key decisions, and manages communication.	Director	Lead Developer	Internal Chat / Mobile
IT / Technical Lead	Performs system restoration, infrastructure failover, and technical validation.	Lead Developer	Director	Internal Chat / Mobile
Support Lead	Manages all	Technical	Lead	Internal Chat /

	customer-facing communication and support channels.	Support Specialist	Developer	Email
Management	Approves escalations, resource allocation, and major external notifications.	Director	Lead Developer	Internal Chat / Mobile

6. Communication Plan

Clear communication is critical during any disruption.

6.1. Internal Communication

- **Response Team:** All incident response communication will be coordinated by the **Incident Lead** via a dedicated channel (e.g., Internal Chat #incident-response).
- **All-Staff Updates:** The Incident Lead will provide status updates to all 2BrightSparks staff via company-wide email or chat every 60 minutes, or as new information becomes available.

6.2. External (Customer) Communication

All external communication is managed by the **Support Lead** and must be approved by the **Incident Lead** or **Management** before release.

External Communication Matrix

Audience	Trigger	Channel	Frequency	Owner
Customers	Initial Incident (Confirmed)	Support Portal Announcement, Website Status Page	Within 1 hour of declaration	Support Lead
Customers	Ongoing	Support	Every 2-4	Support Lead

	Incident	Portal, Website Status Page	hours, or as new info is available	
Customers	Service Restoration	Support Portal, Website Status Page, Email (if needed)	Upon resolution	Support Lead
Stakeholders	Major Incident Declaration	Direct Email / Call	As needed	Management

7. Critical Business Functions & Priorities

Function	**RTO (Recovery Time Objective)**	**RPO (Recovery Point Objective)**	**Notes**
Licensing server availability	4 hours	1 hour	Ensures customers can validate licenses.
Website and downloads	8 hours	4 hours	Public site and installers must remain accessible.
Support ticketing system	12 hours	8 hours	Allows ongoing assistance to customers.
Development environment	24 hours	12 hours	Ensures continuity of development and releases.

8. Systems & Data Protection

- Production systems are hosted in resilient cloud infrastructure with geographically redundant failover capabilities.

- Administrative access is secured using strong authentication and role-based access control.
- Regular automated backups are taken of:
  - Licensing (Customer) database
  - Website and download delivery infrastructure
  - Source code
  - Internal configuration and documentation
- Backups are encrypted and stored in at least two independent regions/providers.

9. Disaster Scenarios & Response

Scenario	Response Actions
Hardware or hosting failure	**Automated using Cloudflare.** Initiate failover to redundant backup hosting. Restore from latest backup if data is affected. (Owner: IT Lead)
Website outage or DNS failure	**Automated using Cloudflare.** Switch DNS to secondary CDN / hosting endpoints. Validate TLS certificates. (Owner: IT Lead)
Licensing service interruption	Activate backup licensing endpoint. Notify customers via Support Lead if manual offline activation is required. (Owner: IT Lead)
Data corruption	Restore from the most recent valid backup. Verify data integrity before re-enabling service. (Owner: IT Lead)
Security breach or compromise	Isolate affected systems immediately. Rotate all credentials. Perform incident response analysis. Notify affected parties if required. (Owner: Incident Lead, IT Lead)

10. Business Continuity During Disruption

- All operations staff are equipped to work remotely and securely from distributed locations.
- Internal communication channels (email, internal collaboration tools) are cloud-based and remain active, independent of primary hosting.

11. Testing & Validation

This plan is validated using the following methods to ensure RTO/RPO objectives are met:

- **Backup Restoration Tests:** (At least semi-annually) A full restoration of all critical databases and systems (as listed in section 8) is performed in a sandbox environment to validate data integrity and restore procedures.
- **Tabletop Exercises:** (Annually) The response team (section 5) walks through a simulated disaster scenario to identify gaps in the plan and confirm roles.
- **Full Failover Tests:** (Annually) A test of critical infrastructure (e.g., Licensing Server failover) is conducted to validate RTOs.
- **Post-Incident Review:** After any real-world activation of this plan, a formal review will be conducted within 14 days to identify lessons learned and update this document.

12. Document Maintenance & Control

This BC/DR plan is a living document. It will be reviewed at least annually, or after any major infrastructure change, to ensure it remains accurate.

Document Version History

Version	Date	Approver	Summary of Changes
1.0	11 Nov 2025	Michael Leaver	Initial formal release. Incorporates new sections for Activation, Communication Plan, and robust Testing procedures.