Business Continuity Plan

Version 1 - Approved by Rishabh

Contents

1. Objective

The objective of this business continuity plan is to prepare Superhawk AI in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible within an acceptable time frame.

2. Scope

The scope of this plan covers business continuity and disaster recovery for Superhawk AI's production services and supporting systems hosted on cloud platforms (primarily AWS and GCP), associated data stored in those environments, and company-managed endpoints (employee laptops/workstations). It includes recovery activities related to services deployed via code stored in GitHub and communications through Google Workspace. This plan does not cover third-party SaaS vendor internal failures beyond their published SLAs except where vendor-managed backup or recovery capabilities are relied upon.

3. Plan Objectives

- Serves as a guide for the recovery teams of Superhawk AI.
- References and points to the location of critical data.
- Provides procedures and resources needed to assist in recovery.
- Identifies vendors and customers that must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing, and reviewing recovery procedures. - Ensure restoration of customer-facing SaaS functionality hosted on AWS and GCP within defined RTOs and with acceptable RPOs.

4. Assumptions

- Key people (team leaders or alternates) will be available following a disaster.
- A national disaster such as a nuclear war is beyond the scope of this plan.
- This document and all vital records are stored in a secure off-site location and not only survive the disaster but are accessible immediately following the disaster.
- Each support organization will have its own plan consisting of unique recovery procedures, critical resource information, and procedures. - Backups for production systems are provided via cloud-provider or managed services (e.g., snapshot, managed database backups) and tested periodically. - Code and deployment artifacts are maintained in GitHub; CI/CD pipelines and deployment configurations are assumed to be recoverable from those repositories. - Incident notifications and stakeholder communications leverage Google Workspace and internal on-call/alerting tools.

5. Disaster Definition

Any loss of utility service (power, water), connectivity (system sites), or catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided by Superhawk AI operations. The plan identifies vulnerabilities and recommends measures to prevent extended service outages.

6. Preparation for Disaster Recovery & Business Continuity

- It is essential that frequent backups are taken, and backups are stored at a redundant location to facilitate restoration in case of a disaster.
- A backup restoration exercise should be performed by the Infra Operations Person with help from the engineering team.
- The Information Security Officer should ensure that a disaster recovery mock drill is conducted by the Engineering team, which will then allow them to invoke this plan effectively. This exercise may be a tabletop exercise based on the availability commitments.
- If required, through the disaster recovery exercise, the Engineering team should evaluate the following:
    - Recovery time objective
    - Recovery point objective - Backup responsibilities: cloud infrastructure backups (snapshots, managed DB backups) are managed using AWS/GCP native services or approved managed services; employee device backups are the responsibility of individual users with guidance from IT. Where vendor-managed backups are used, the organization will maintain documentation of vendor backup configurations and retention settings. - Testing cadence: full restore drills of critical services shall be performed at least annually; incremental or tabletop exercises shall be performed quarterly or after significant changes to infrastructure or applications. - Runbooks: Engineering maintains runbooks stored in the approved documentation repository that detail recovery steps for critical services, access procedures for AWS and GCP consoles, and GitHub repository recovery steps.

7. Instructions for Using the Plan

7.1 Invoking the Plan

This plan becomes effective when a disaster occurs.

7.2 Disaster Declaration

The Information Security Officer and/or Engineering Head is responsible for declaring a disaster and activating the various recovery teams as outlined in this plan.

In a major disaster situation affecting multiple business units, the decision to declare a disaster will be determined by senior management. The Engineering Team will respond based on the directives specified by senior management.

7.3 Plan Review & Maintenance

This document and the disaster recovery mock drill must be reviewed at least once annually.

7.4 Notification of Incident/Disaster

- In cases of technical incidents, the Infra Operations Person/On-Call Engineer personnel should contact the Information Security Officer.

- For any operational incident, it is the responsibility of the user/employee to report it as soon as possible through the Sprinto App and/or other means like e-mail or telephone, as applicable. These incidents should be reviewed and resolved in accordance with the Incident Management Policy, and notification must be made to the Information Security Officer.
- The Information Security Officer should be notified promptly when any of the following conditions exist:
    - Any security incident
    - Any server is down for three or more hours.
    - Any problem at any system that would cause the above condition to be present or there is a certain indication that the above condition is about to occur.
- The Information Security Officer should contact the respective Superhawk AI Business heads and report that a disaster has taken place.
- Once a disaster has been declared, it must follow the incident management procedure and change management procedures while trying to bring back the availability of services.
- Declare a disaster only if the situation is not likely to be resolved within predefined time frames. The person who is authorized to declare a disaster must also have at least one backup person who is also authorized to declare a disaster in the event the primary person is unavailable.
- It is the responsibility of the Information Security Officer to ensure the event of a disaster and the successful recovery are communicated to relevant stakeholders, customers, and regulatory bodies as applicable. - Communication channels: initial internal alerts and coordination will use Google Workspace (email, Google Meet) and the company's on-call alerting mechanism; customer notifications will follow pre-approved templates and channels as defined by the Communications lead.

8. Document Security Classification

Company Internal. Please refer to the Data Classification Policy for more details.

9. Non-Compliance

Compliance with this policy shall be verified through various methods, including, but not limited to, automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, which may include termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

10. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation. Additional responsibilities:

- Engineering/Infra: maintain cloud infrastructure recovery runbooks, execute backup restores, and perform annual recovery drills for AWS and GCP-hosted services.

- On-Call/Infra Operations: monitor alerts, initiate incident notifications, and perform first-response mitigation.
- IT/Endpoint Support: maintain guidance for employee device recovery and secure configuration for laptops/workstations.
- Communications/Business Heads: coordinate external communications to customers and regulators during and after a declared disaster.

11. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization, including changes to cloud providers (AWS, GCP), core architecture, or major third-party vendor relationships. Recovery drills and backup restore tests shall be scheduled and documented annually, with records retained per the Records Retention Policy.

End of Business Continuity Plan. For version history, please see the next page.

Version History

	Version	Log	Date
1	Current	Policy version approved by Rishabh	13 Mar, 2026
1		New policy version created	13 Mar, 2026