Business Continuity & Disaster Recovery Policy

Version 2 - Approved by Tahmid Awal

Company Internal
Created on sprinto.com

Contents

1. Objective
2. Scope
3. Policy statement
4. Information Security Aspect of Business Continuity Management
5. Document Security Classification
6. Non-Compliance
7. Responsibilities
8. Schedule
9. Version History

1. Objective

The objective of this policy is to provide guidelines for PlanSyncAI's business continuity and disaster recovery. The document prescribes the requirements to plan for recovery during disasters so that business commitments to customers can always be met.

2. Scope

This document is applicable to all processes and operations in PlanSyncAI within the scope of the ISMS.

3. Policy statement

PlanSyncAI is committed to ensuring the highest level of service to its customers. Thus continuity of operations in a secure manner must be planned for and embedded in the organization's business continuity management and disaster recovery planning activities.

4. Information Security Aspect of Business Continuity Management

4.1 Information Security Continuity

4.1.1 Planning Information Security Continuity

- The organization-wide information security processes shall include Information Security requirements to help ensure that confidentiality, integrity, and availability of critical information assets shall be preserved even in the event of a business disruption or disaster.
- PlanSyncAI shall identify recovery guidelines that can be taken as a baseline reference to classify mission-critical systems and develop recovery and restoration plans.
- A strategy plan shall be developed for the overall business continuity/disaster recovery approach. Information security controls applicable during BAU (Business as usual) scenarios shall be relevant even during disaster scenarios. All exceptions shall need approval from the Information Security Officer and senior management.
- The organization ensures ICT readiness through the implementation of robust disaster recovery and business continuity measures, including regular data backups, system redundancy, and failover capabilities. Critical systems are protected by automated monitoring, incident response procedures, and recovery strategies that ensure minimal downtime. These measures are regularly tested through simulations and audits, reviewed for continuous improvement, and updated to maintain resilience and availability of essential services in alignment with compliance requirements.

4.1.2 Implementing Information Security Continuity

- PlanSyncAI shall ensure that an adequate framework is in place to prepare for, mitigate, and respond to a disruptive event using personnel with the necessary authority, experience, and competence.

- PlanSyncAI shall identify personnel with the necessary responsibility, authority, and competence to manage an incident and maintain information security.
- PlanSyncAI should consider the development and approval of comprehensive and well-documented plans, response strategies, and recovery procedures to effectively manage and mitigate the impact of any potential disruptive event.

4.1.3 Verify, Review & Evaluate Information Security Continuity

- Information security controls for all business continuity sites and systems shall be reviewed and verified. Business continuity plans shall be tested and updated regularly to ensure they are up to date and effective.
- The roles and responsibilities for both information systems' contingency planning and recovery shall be reviewed and updated at least annually.

4.2 Redundancies

- PlanSyncAI shall identify business requirements for the availability of information systems.
- Redundant components or architectures shall be considered wherever availability cannot be guaranteed using the existing systems architecture.
- Redundant information systems shall be tested to ensure the successful failover from one component to another.

5. Document Security Classification

Company Internal (please refer to the Data Classification policy for more details).

6. 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.

7. 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.

8. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of Business Continuity & Disaster Recovery Policy. For version history, please see the next page.

Version History

Version		Log	Date
2	Current	Policy version reviewed by Cameron Abernethy	04 Aug, 2026
2		Policy version reviewed by Cameron Abernethy	02 Jul, 2025
2		Policy version approved by Tahmid Awal	30 Jun, 2025
2		New policy version created	30 Jun, 2025
1		Policy version approved by Tahmid Awal	23 Jun, 2025
1		New policy version created	23 Jun, 2025