



ECOSYN FOUNDATION

FOUNDATION GOVERNANCE DOCUMENT

BUSINESS CONTINUITY PLAN

Continuity, crisis response and recovery framework

Version 1.0 | Board adoption draft
The Netherlands | 14 June 2026

Document Control

Document title	Business Continuity Plan
Organization	ECOSYN Foundation
Document owner	Board of Directors / Operations Lead
Version / status	Version 1.0 / Board adoption draft
Date	14 June 2026
Governing framework	Applicable law, the Articles of Association, board resolutions and internal policies of the Foundation.

Contents

1	Purpose and status
2	Critical activities
3	Risk scenarios
4	Continuity strategy
5	Recovery priorities and target times
6	Incident activation and decision-making
7	Communication plan
8	Testing, training and review
9	Final Statement

This table of contents is a static guide. Page numbers may be generated or updated in Microsoft Word if required.

1. Purpose and status

This Business Continuity Plan defines how ECOSYN Foundation will maintain or restore essential activities during disruptions. It replaces the business-service and securities-focused wording of the source document with a foundation-oriented framework.

- 1.1 The plan applies to governance, donor and stakeholder communication, project administration, finance, records, website availability, events, field activities, data protection and crisis response.
- 1.2 The plan is operational rather than absolute. It sets target procedures and recovery priorities but does not guarantee uninterrupted availability of systems, services or third-party infrastructure.
- 1.3 The Foundation shall review this plan at least annually and after any major incident, significant organizational change or change in critical suppliers.

2. Critical activities

- 2.1 Critical activities include board decision-making, legal and compliance records, accounting records, donation and grant administration, payment approvals, project files, beneficiary and stakeholder communications, data protection obligations, public website notices and emergency contact capability.
- 2.2 Essential records include the Articles of Association, board resolutions, contracts, insurance documents, financial records, donation records, employment or volunteer records, project documentation, IT access lists and emergency contacts.
- 2.3 Each critical activity shall have a responsible owner, a deputy owner, a minimum operating procedure and a location where current recovery information is stored.

3. Risk scenarios

- 3.1 The Foundation prepares for disruption scenarios including loss of office access, staff or volunteer unavailability, cyber incident, data loss, website outage, payment-system failure, power or network outage, supplier failure, travel or event disruption, natural disaster and reputational crisis.
- 3.2 Risk assessments shall consider likelihood, impact, legal obligations, personal-data exposure, financial exposure, safety exposure and reputational consequences.
- 3.3 Risks that may affect people, personal data, money or public trust shall be escalated to the Board or a delegated continuity officer without delay.

4. Continuity strategy

- 4.1 Where feasible, the Foundation shall maintain secure remote-working capability for board members and essential staff or collaborators.
- 4.2 Critical data shall be stored in managed systems with access control, backup, recovery capability and documented administrator access.
- 4.3 The Foundation shall maintain at least one alternative communication channel for urgent notices, such as secondary email, secure messaging, telephone contact lists or website status notices.
- 4.4 For critical suppliers such as hosting, accounting, email, payment and cloud-storage providers, the Foundation shall record support contacts, contract references and basic recovery steps.
- 4.5 The Foundation shall keep enough documentation outside a single physical location to enable operations to resume if the main office, device or account is unavailable.

5. Recovery priorities and target times

- 5.1 Immediate priority: protect people, preserve evidence, secure funds, secure personal data and stop further loss.

- 5.2** Recovery within 24 hours should target board contact capability, emergency communications, basic email access, critical passwords through approved recovery procedures, payment freeze or approval controls if needed, and public notice if services are affected.
- 5.3** Recovery within 72 hours should target project coordination, donor or partner updates, financial workflow, document access, event decisions and supplier escalation.
- 5.4** Recovery within 7 days should target full administrative capacity, incident report completion, root-cause analysis and implementation of corrective measures.
- 5.5** Where a different recovery objective is required by contract, law or donor agreement, that stricter requirement shall apply.

6. Incident activation and decision-making

- 6.1** The plan may be activated by the Board, the Chair/President, the Executive Director, the Operations Manager or another person expressly delegated by the Board.
- 6.2** An incident log shall be opened for any material disruption. The log records time, facts known, decisions, responsible persons, communications, affected systems, financial exposure and follow-up actions.
- 6.3** Urgent decisions may be taken by the smallest available authorized group when delay would create legal, financial, safety or data-protection risk. Such decisions shall be reported to the Board as soon as practicable.
- 6.4** The Foundation shall avoid speculative public statements. Public communications must be factual, proportionate and approved by an authorized person.

7. Communication plan

- 7.1** The Foundation shall maintain current contact lists for board members, key staff, volunteers, project leads, IT providers, banking contacts, insurers, legal advisers and critical partners.
- 7.2** During a disruption, communications shall identify the nature of the disruption, the expected impact, temporary procedures, contact points and estimated next update time.
- 7.3** When personal data may be affected, communications shall be coordinated with the person responsible for privacy compliance and handled in accordance with applicable data-protection rules.
- 7.4** Stakeholders shall be informed only to the extent necessary and appropriate. Sensitive operational, security or personal information shall not be disclosed publicly.

8. Testing, training and review

- 8.1** The Foundation shall test essential recovery procedures at least annually. Testing may include backup restore, emergency contact checks, simulated website outage, payment approval continuity or tabletop crisis exercises.
- 8.2** Findings from tests and incidents shall be documented, assigned to responsible persons and tracked until resolved.
- 8.3** New board members, relevant staff and relevant volunteers shall receive basic continuity and incident-reporting instructions.
- 8.4** The Board shall approve material changes to this plan.

Final Statement

This document is intended to be adopted, amended or withdrawn by the competent body of ECOSYN Foundation. If any provision conflicts with mandatory law, the Articles of Association or a valid board resolution, the stricter or higher-ranking rule shall prevail.

Copyright © ECOSYN Foundation. All rights reserved. Reproduction, adaptation or distribution outside authorized use requires prior written permission, except where permitted by law.

***** END OF DOCUMENT *****