ECOSYN FOUNDATION

FOUNDATION GOVERNANCE DOCUMENT

SECURITY AND PROTECTION RULES

Security, safety, cybersecurity and incident-response procedures

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

Document Control

Document title	Security and Protection Rules
Organization	ECOSYN Foundation
Document owner	Board of Directors / Security or 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 scope
2	Security governance and risk levels
3	Physical security and events
4	Travel and field activities
5	Cybersecurity and access control
6	Data and communication protection
7	Equipment, documents and assets
8	Incident reporting and response
9	Training and awareness
10	Violations and sanctions
11	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 scope

These Security and Protection Rules define practical measures to protect people, information, funds, equipment, events and the reputation of ECOSYN Foundation. The wording has been adapted away from diplomatic and weapons-oriented language toward foundation operations, events, travel, cybersecurity and incident management.

1.1 The Rules apply to board members, officers, employees, volunteers, project participants, consultants, visitors, collaborators and third parties using Foundation systems or attending Foundation activities.

1.2 The Rules cover physical security, event security, travel safety, cybersecurity, data protection, access control, equipment, emergency response and incident reporting.

1.3 Security measures must be lawful, proportionate, risk-based and respectful of human rights and privacy.

2. Security governance and risk levels

2.1 The Board may appoint a security officer, operations officer, IT administrator or incident lead responsible for implementing these Rules.

2.2 The Foundation may classify risk as low, medium or high based on threat level, location, activity, public exposure, data sensitivity, financial exposure and vulnerable persons involved.

2.3 High-risk activities require a documented risk assessment and approval by an authorized person before commencement.

2.4 Security procedures shall be reviewed after incidents, before major events and when the threat environment changes.

3. Physical security and events

3.1 Event organizers must assess venue access, emergency exits, crowd size, first-aid arrangements, fire safety, participant registration, sensitive guests, media exposure and incident response.

3.2 Access to restricted areas, records, storage, devices and financial materials must be limited to authorized persons.

3.3 Identification badges or sign-in procedures may be used at official events where appropriate.

3.4 Participants must follow venue rules and instructions issued by authorized Foundation representatives.

3.5 Threats, violence, harassment, stalking, theft, vandalism, unauthorized recording in restricted areas and disruptive behaviour must be reported and may lead to removal from the activity.

4. Travel and field activities

4.1 Before travel or field activity, the responsible lead shall consider destination risk, local laws, emergency contacts, health and safety, insurance, transport, communications, data protection and contingency options.

4.2 High-risk travel requires approval, a contact plan, check-in procedure and emergency escalation contact.

4.3 Participants must comply with local law and safety instructions and must not expose beneficiaries, staff, volunteers or partners to unnecessary risk.

4.4 Where professional security support is required, it must be engaged lawfully, contractually and under Board-approved parameters.

4.5 The Foundation does not authorize weapons, armed activity or security measures except where expressly lawful, necessary, carried out by properly licensed professionals and approved in writing by the Board.

5. Cybersecurity and access control

5.1 Foundation systems must use strong passwords, multi-factor authentication where available, role-based access, secure backups and prompt removal of access when a role ends.

5.2 Administrative accounts must be limited to persons who need them and must not be shared.

5.3 Devices used for Foundation work should be updated, protected against malware, secured by screen lock and encrypted where appropriate.

5.4 Suspicious emails, links, attachments, login alerts, unexpected payment changes or suspected phishing must be reported promptly.

5.5 Website, email, cloud storage, payment and accounting accounts must have documented recovery procedures and current administrator contact details.

6. Data and communication protection

6.1 Confidential information and personal data must be transmitted and stored only through approved channels appropriate to the sensitivity of the information.

6.2 Sensitive documents should not be sent to personal accounts or stored on unmanaged devices unless specifically authorized and secured.

6.3 Public communication must avoid revealing private addresses, personal data, security arrangements, passwords, confidential partners, vulnerable beneficiaries or details that could enable misuse.

6.4 Data incidents, including lost devices, misdirected emails, unauthorized access, ransomware, leaked documents and suspected hacking, must be treated as security incidents.

7. Equipment, documents and assets

7.1 Foundation equipment, documents, seals, certificates, badges, access cards, keys, phones, laptops, storage media and vehicles must be protected from loss, misuse and unauthorized access.

7.2 Loss or damage must be reported promptly with details of what was lost, when, where, who may be affected and what immediate steps were taken.

7.3 Sensitive physical documents must be stored securely and destroyed securely when disposal is authorized.

7.4 Equipment issued to a person must be returned when the role, project or authorization ends.

8. Incident reporting and response

8.1 Security incidents must be reported immediately to the designated contact, operations lead, IT administrator or Board member.

8.2 An incident report should record the facts known, time, location, persons involved, systems affected, data affected, financial exposure, immediate actions and proposed next steps.

8.3 The Foundation shall preserve evidence, contain the risk, protect affected persons, notify relevant authorities where required and communicate proportionately with stakeholders.

8.4 Where a personal-data breach may have occurred, the incident must be escalated to the privacy responsible person without delay.

8.5 After a material incident, the Foundation shall conduct a lessons-learned review and implement corrective measures.

9. Training and awareness

9.1 Relevant persons shall receive basic security instructions appropriate to their role.

9.2 Training may include phishing awareness, password hygiene, event safety, travel safety, first aid, data protection, incident reporting and safeguarding.

9.3 High-risk roles or activities may require additional training or written acknowledgment of security procedures.

9.4 Security instructions must be practical, current and proportionate to the Foundation's size and activities.

10. Violations and sanctions

10.1 A breach of these Rules may result in warning, retraining, restriction of access, removal from activity, suspension, termination of role or contract, recovery of losses or referral to competent authorities.

10.2 Serious breaches include deliberate unauthorized access, theft, violence, harassment, misuse of credentials, concealment of a data incident, disclosure of confidential information, fraud or reckless disregard of safety instructions.

10.3 Access may be suspended immediately where necessary to protect people, data, funds, systems or assets while a matter is reviewed.

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.

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