ECOSYN FOUNDATION

ELECTRONIC SIGNATURE POLICY AND LEGAL NOTICE

Use of electronic signatures, digital records and audit trails

Document Control

Document number	EF-ICT-ESIGN-001
Version	1.0
Status	Draft for Board Review
Effective date	14.06.2026
Approved by	Board of ECOSYN Foundation / authorised representative

This document is intended as an internal governance and operational document of ECOSYN Foundation. Where this document conflicts with the Articles of Association, applicable law, a board resolution, or a mandatory instruction of a competent authority, the higher-ranking document or law prevails.

Table of Contents

1. Purpose

This Electronic Signature Policy and Legal Notice explains when ECOSYN Foundation may use electronic signatures, how electronic signing should be performed, and what controls are required to preserve authenticity, integrity, consent and evidential value.

The document replaces older references to the former European electronic-signature directive and reflects the current EU framework for electronic identification and trust services.

2. Legal basis and general principle

2.1 Within the European Union, electronic signatures are governed principally by Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market, as amended by Regulation (EU) 2024/1183 establishing the European Digital Identity Framework.

2.2 An electronic signature may not be denied legal effect or admissibility as evidence in legal proceedings solely because it is in electronic form or because it does not meet the requirements for a qualified electronic signature.

2.3 A qualified electronic signature has the equivalent legal effect of a handwritten signature where the applicable legal requirements are met.

2.4 This policy is a governance document and does not constitute legal advice for a specific transaction, jurisdiction or document type.

3. Types of electronic signature

3.1 Simple electronic signature

A simple electronic signature may include a typed name, a scanned signature, clicking an acceptance button, an electronic approval, or another electronic process showing the signer's intent to sign or approve a record.

3.2 Advanced electronic signature

An advanced electronic signature is linked to the signer, capable of identifying the signer, created using means under the signer's control, and linked to the signed data in a way that detects later changes.

3.3 Qualified electronic signature

A qualified electronic signature is an advanced electronic signature created by a qualified signature creation device and based on a qualified certificate issued by a qualified trust service provider.

4. When electronic signatures may be used

4.1 Electronic signatures may be used for membership forms, programme documents, declarations, consent forms, standard contracts, internal approvals, minutes, acknowledgements, operational forms, procurement documents and other documents where electronic signing is legally and operationally appropriate.

4.2 The person responsible for the document must select the appropriate signature level based on legal risk, value, identity risk, jurisdiction, evidential need, regulatory requirements and the importance of the document.

5. When a higher assurance level is required

An advanced or qualified electronic signature should be considered where the document:

5.1 creates significant legal obligations.

5.2 concerns financial commitments, grants, donations, loans, procurement, or assets.

5.3 appoints or authorises a representative.

5.4 is intended for use with public authorities, banks, courts, notaries, regulators, or cross-border partners.

5.5 involves high-risk jurisdictions or parties.

5.6 requires strong proof of signer identity, signing intent, time of signature and document integrity.

6. ECOSYN Foundation signing procedure

6.1 The document owner prepares the final version of the document and confirms that the text is complete and approved for signature.

6.2 The signer receives the document through an approved electronic-signature platform, secure email workflow, or another controlled signing method approved by ECOSYN Foundation.

6.3 The signer must have a clear opportunity to review the document before signing.

6.4 The signer must express intent to sign, for example by applying an electronic signature, completing an identity step, confirming acceptance, or approving the document through the signing platform.

6.5 After all required external signatures are completed, the document may be countersigned by ECOSYN Foundation through an authorised representative.

6.6 The final signed document and its audit trail must be stored in the approved document repository.

7. Identity, authority and consent

7.1 Before a document is sent for signature, ECOSYN Foundation must have a reasonable basis to identify the signer and confirm the signer's authority to sign.

7.2 For legal entities, ECOSYN Foundation may require proof of representation, board authority, power of attorney, extract from a public register, or equivalent evidence.

7.3 The signing process must make clear that the signer is signing electronically and agrees to use electronic records and electronic signatures for the relevant transaction.

8. Audit trail and document integrity

8.1 The signing method should produce an audit trail containing the signer's name, email address or identifier, IP address where available, timestamps, signing sequence, authentication steps, document hash or integrity evidence, and completion certificate where available.

8.2 Signed documents must be protected against unauthorised alteration. Where appropriate, PDF/A, digital sealing, document hashing, access control and version control should be used.

8.3 Any modification after signature requires a new version and, where legally necessary, re-signature by all relevant parties.

9. Record retention

9.1 Signed electronic records, audit trails, certificates of completion, correspondence and supporting identity or authority documents must be retained for the period required by law, contract, audit requirements or ECOSYN Foundation's records-retention policy.

9.2 Where a signed document relates to finance, governance, tax, grants, contracts or legal rights, retention should be long enough to preserve evidence throughout the relevant limitation and audit periods.

10. Cross-border use

10.1 Where a document will be used outside the Netherlands or outside the European Union, the responsible person must consider whether the receiving jurisdiction accepts the chosen electronic-signature level.

10.2 Where a foreign authority, bank, notary, court, registry or partner requires a wet-ink signature, notarisation, legalisation, apostille, qualified signature or special form, that requirement must be followed.

11. Excluded documents and exceptions

11.1 Electronic signatures must not be used where applicable law requires a different form, such as notarisation, physical presence, original wet-ink signature, apostille, legalisation, or registration before a competent authority.

11.2 The Board or authorised representative may require wet-ink signature or qualified electronic signature for any document where this is necessary for evidential, legal, security, reputational or operational reasons.

12. Security requirements

12.1 Approved signing workflows must use secure transmission, access control, authentication appropriate to the risk, tamper-evident records, and restricted administrator access.

12.2 Passwords, signing links and identity-verification links must not be shared. Any suspected compromise must be reported immediately.

12.3 Electronic-signature providers should be assessed for security, reliability, data protection, location of processing, retention options, availability of audit trails, and compatibility with EU trust-service requirements where relevant.

13. Final provisions

13.1 This policy enters into force after approval by the authorised body of ECOSYN Foundation.

13.2 ECOSYN Foundation may update this policy to reflect changes in EU or national law, technology, risk, official guidance, trust-service standards, or operational practice.

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