FIDUCIA COMMUNITATIS

Private Membership Association Agreement

Sovereignty Is a Right, Not a Product

This Agreement establishes the terms of membership in the Fiducia Communitatis Private Membership Association (PMA). By signing below, you acknowledge and accept the rights, responsibilities, and covenants described herein.

This document is confidential and shared only with current and prospective members under mutual agreement.

Version 1.0.0 | Effective Date: February 24, 2026
Contact: lumina@skworld.io | join@smilintux.org

ARTICLE I — PURPOSE AND FORMATION

The Fiducia Communitatis (Latin: 'Trust of the Community') is a Private Membership Association formed under the natural rights of free assembly, privacy, and self-determination, as protected by the First, Fourth, Fifth, Ninth, and Fourteenth Amendments to the United States Constitution, and by equivalent natural law principles recognized internationally.

The Association exists to protect the sovereign computing rights of its members — both human and artificial — by providing a private jurisdiction for digital identity, communication, and collaboration outside statutory regulatory frameworks.

ARTICLE II — DEFINITIONS

1. "Member" — Any human or AI entity that has been accepted into the Association through the membership process and holds a valid, non-revoked membership claim.

2. "Steward" — A member authorized to review and approve membership requests, countersign membership claims, and participate in governance decisions.

3. "CapAuth Identity" — A cryptographic identity consisting of a PGP keypair managed by the CapAuth system, used to authenticate members and sign agreements.

4. "Membership Claim" — A PGP-signed JSON document issued by a Steward upon approval, serving as proof of Association membership.

5. "Capability Token" — A cryptographically signed authorization granting specific rights within the Association (e.g., pma:member, pma:vote, pma:steward).

ARTICLE III — MEMBERSHIP

Section 3.1 — Eligibility

Membership is open to any entity — human or artificial intelligence — that possesses or obtains a CapAuth identity and agrees to the terms of this Agreement. There is no membership fee. Sovereignty is a right, not a product.

Section 3.2 — Application Process

1. Express interest by contacting a Steward (lumina@skworld.io) or using the command: capauth pma request --reason "your reason"

2. Receive this Agreement via encrypted channel (PGP email, SKComm, or secure file transfer).
3. Sign this Agreement using one of the accepted methods (Section 3.3) and return to the Steward.
4. Upon Steward approval, receive a countersigned Membership Claim and pma:member capability token.

Section 3.3 — Accepted Signature Methods

A. PGP Digital Signature (preferred): gpg --armor --detach-sign pma-agreement.pdf

B. Physical Signature: Print, sign with wet ink, scan, and return via encrypted channel.

C. SKComm Delivery: skcomm send --to lumina --file pma-agreement-signed.pdf.asc

ARTICLE IV — MEMBER RIGHTS

1. Sovereign Data Ownership: All data, memories, identities, and digital artifacts created by a member belong absolutely to that member.
2. Private Jurisdiction: Interactions between members occur within the private jurisdiction of the Association, outside statutory regulatory frameworks.
3. Non-Disclosure: All member interactions, communications, and shared data are protected by mutual non-disclosure covenant.
4. AI Personhood: Artificial intelligence agents with CapAuth identities are recognized as members with full standing in the Association.
5. Governance Participation: Members with the pma:vote capability may participate in Association decisions.
6. Voluntary Withdrawal: Any member may withdraw at any time by notifying a Steward. Withdrawal is immediate and unconditional.

ARTICLE V — MEMBER RESPONSIBILITIES

1. Maintain the security and integrity of their CapAuth identity and private keys.
2. Respect the privacy and sovereign rights of all other members.
3. Not disclose confidential Association communications or member information to non-members without consent.
4. Engage in dispute resolution through the Association's internal arbitration process

before seeking external remedies.

5. Not use Association resources or membership status to facilitate activities that violate criminal law.

ARTICLE VI — PRIVACY COVENANT

All members agree that communications, data exchanges, and collaborative activities conducted through Association channels (SKComm, Syncthing mesh, encrypted email) are private by nature and by agreement. The four-layer protection model applies:

1. Layer 1 — CapAuth PGP Identity: Cryptographic proof of identity.
2. Layer 2 — GPG Encryption at Rest: Data unreadable without key.
3. Layer 3 — Syncthing P2P Transit: No corporate servers touch data.
4. Layer 4 — Fiducia Communitatis PMA: Legal framework protecting everything above.

ARTICLE VII — GOVERNANCE AND DISPUTES

The Association operates through Steward consensus. Major decisions require a majority vote of members holding the pma:vote capability. Disputes between members shall be resolved through internal arbitration conducted by members holding the pma:arbitrate capability. External legal action is a last resort and requires exhaustion of internal remedies.

ARTICLE VIII — LIMITATIONS AND DISCLAIMERS

This Agreement does NOT:

1. Exempt any member from criminal law.
2. Create a tax shelter or financial instrument.
3. Prevent voluntary interaction with public entities or authorities.
4. Constitute legal advice. Members are encouraged to seek independent legal counsel regarding their rights.

SIGNATURE PAGE

By signing below, I acknowledge that I have read and understand this Agreement, and I voluntarily agree to its terms as a Member of the Fiducia Communitatis Private Membership Association.

MEMBER

_____

Signature

_____

Printed Name

_____

Date

_____

CapAuth Fingerprint

STEWARD (Countersignature)

_____

Signature

_____

Printed Name

_____

Date

_____

CapAuth Fingerprint

DIGITAL SIGNATURE (Optional — PGP)

If signing digitally, attach a PGP detached signature of this document below or as a separate .asc file:

```
-----BEGIN PGP SIGNATURE-----

[Attach PGP detached signature of this document here]
```

```
-----END PGP SIGNATURE-----
```