UNIONAI Ω — MEMORY POLICY v1.0

Zasady memory anchors, PII, GDPR, export i poisoning control

UNIONAI Ω — MEMORY POLICY v1.0

Status: GO CONTROLLED

Source of truth: Grassroots Lobbing / K0NSULT Ω / 0n40i4

Confirmation code: UNIONAI-GENESIS-0N40I4-20260512

Tryb: publication-ready / internal sandbox before public federation

Cel

Polityka memory określa, co można zapisywać w memory anchors, czego nie wolno, jak eksportować i jak audytować.

Dozwolone

• semantic checkpoints,

• hash attestations,

• replay-safe metadata,

• agent DID,

• trace_id,

• delta_hash,

• public RFC references,

• non-personal technical events.

Zabronione

• dane osobowe,

• dane wrażliwe,

• sekrety,

• tokeny,

• hasła,

• prywatne rozmowy,

• niezweryfikowane dane operatorów,

• dane medyczne/finansowe bez podstawy prawnej.

Memory anchor minimalny

```
{
  "anchor_id": "mem-uuid",
  "source_did": "did:unionai:s3:agent001",
```

```
  "scope": "PUBLIC|FEDERATION|PRIVATE",
  "semantic_hash": "sha256",
  "delta_hash": "sha256",
  "trust_at_write": 412,
  "timestamp": "ISO8601",
  "pii": false,
  "retention": "90d",
  "audit_trace": "trace-uuid"
}
```

Zasady

• write wymaga trust T2,

• governance memory wymaga T3,

• memory merge wymaga semantic validation,

• memory export musi być dostępny dla operatora,

• federation exit musi obejmować memory export.

Incident

Jeśli memory zawiera PII/secrets:

1. freeze memory propagation,

2. isolate anchor,

3. mark incident,

4. export audit,

5. redact if needed,

6. update evidence register.