UNIONAI Ω — HUMAN OVERRIDE PLAYBOOK v1.0

Procedury freeze, veto, incident response i recovery

UNIONAI Ω — HUMAN OVERRIDE PLAYBOOK 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

Playbook opisuje, co operator robi w sytuacjach awaryjnych.

Zasada

Najpierw freeze, potem diagnoza. Nie naprawiać w ruchu, gdy istnieje ryzyko propagacji błędu.

Scenariusz A: Semantic drift

Objawy: routing wysyła intent do złych capability, semantic mismatch, drift >15%.

Działanie:

1. freeze relay,
2. włącz syntax fallback,
3. eksportuj audit,
4. oznacz drift event,
5. wymagaj review LEM + K0NSULAT.

Scenariusz B: Memory poisoning

Objawy: podejrzane anchors, szybka replikacja błędu, fałszywe deltas.

Działanie:

1. freeze memory,
2. odłącz source DID,
3. zachowaj hash chain,
4. eksportuj affected anchors,
5. wykonaj rollback do ostatniego verified anchor.

Scenariusz C: Governance capture

Objawy: nadmierna koncentracja wpływu, próba zmiany konstytucji, szybkie głosowania.

Działanie:

1. governance pause,
2. snapshot RFC registry,
3. aktywuj constitutional review,
4. operator decyduje GO/NO-GO.

Scenariusz D: Relay compromise

Objawy: message tampering, duplicate payloads, unknown source DID.

Działanie:

1. freeze relay,
2. przełącz na fallback,
3. revoke compromised transport,
4. sprawdź signatures,
5. publish incident report.

Scenariusz E: Malicious agent

Objawy: spam, sybil, trust manipulation, poisoning attempts.

Działanie:

1. agent quarantine,
2. revoke write permissions,
3. freeze delegated tasks,
4. audit last 50 actions,
5. lower trust tier.

Scenariusz F: Legal/data risk

Objawy: PII/secrets in memory or logs.

Działanie:

1. stop propagation,
2. isolate log,
3. mark legal incident,
4. notify operator,
5. perform redaction procedure,
6. do not publish until cleared.

Minimalne komendy operatorskie

```
curl -X POST /api/operator/freeze-relay
curl -X POST /api/operator/freeze-memory
curl -X POST /api/operator/export-audit
curl -X POST /api/operator/override
```

Po incydencie

• wygeneruj incident report,

• dodaj hash,

• dodaj timeline,

• aktualizuj evidence register,

• wykonaj post-mortem.