The F.I.E.L.D. Framework

A company-standard governance layer for agentic AI. FIELD addresses the three concerns that runtime prompt protocols alone cannot: agentic harnessing (how autonomous agents are controlled), AI sovereignty (who owns and authorizes them), and AI federation (how they interoperate across trust boundaries). Where FORCE constrains what an AI says, FIELD constrains how an AI is deployed and accountable.

F — Federation

Purpose. Agents from different organizations, ownership structures, or trust domains must interoperate without leaking authority. Federation defines the trust protocols, contract semantics, and boundary controls that let agents work across sovereign lines without collapsing into a single trust pool.

MANIFEST ENTRY

```
"federation: { trust_boundary: 'spin-state-labs', allowed_peers: ['stripe.com', 'anthropic.com'], contract_schema: 'agent-mcp-v1' }"
```

I — Identity

Purpose. Every autonomous agent represents a principal — a human or organization whose interests it serves. Identity nails down attribution: who owns this agent, whose data does it touch, whose reputation is on the line, whose jurisdiction governs its operation.

MANIFEST ENTRY

```
"identity: { principal: 'don@spinstatelabs.ca', org: 'spin-state-labs', jurisdiction: 'CA-ON', data_scope: 'client-tier-A' }"
```

E — Enforcement

Purpose. Autonomous agents need brakes and rails. Enforcement defines the runtime harnessing: kill switches for immediate halt, action boundaries the agent structurally cannot cross, escalation triggers that pause for human review, rate limits and spend ceilings, reversibility rules for one-way operations.

MANIFEST ENTRY

```
"enforcement: { kill_switch: '/admin/halt', spend_cap_usd: 500, escalation_triggers: ['pii_access', 'external_send'], irreversible_actions: ['deploy', 'delete'] }"
```

L — Ledger

Purpose. If it isn't logged, it didn't happen — and if the record can be rewritten, the audit is theatre. Ledger writes a cryptographic immutable audit trail of every decision, action, delegation event, and refusal. Tamper-evident sealing means neither the agent nor the operator can rewrite history after the fact.

MANIFEST ENTRY

```
"ledger: { store: 's3://spin-state-audit/prod', retention_days: 2555, cryptographic_seal: true, seal_algorithm: 'sha256-chained', includes: ['decisions', 'delegations', 'refusals'] }"
```

D — Delegation

Purpose. Autonomous agents act on behalf of humans. Delegation makes the authorization chain explicit — what actions has this agent been delegated authority to perform, by whom, within what scope, revocable when. Without a clear delegation chain, there is no sovereignty; the agent is a black box acting in someone's name.

MANIFEST ENTRY

```
"delegation: { granted_by: 'cfo@client.com', scope: 'read_gl,post_je<10k', valid_until: '2026-12-31', revocation_url: '/admin/revoke/xyz' }"
```

MISSION STATEMENT — GOVERNANCE, NOT SUGGESTION

"FIELD is the governance manifest for an autonomous agent. (F) Declare the federation boundary and trusted peers. (I) Pin the identity of the principal the agent represents. (E) Wire the enforcement mechanisms — kill switch, spend caps, escalation. (L) Point at the immutable ledger where every action lands. (D) Bind the delegation chain from human to agent, scoped and revocable. Every agent that ships from Spin State Labs carries a FIELD manifest. No manifest, no deploy."