FlowForge Company Plan (Simple Version)

Updated: 2026-02-21   **Audience:** first-time readers   **Read time:** 5-8 minutes

1) What FlowForge Is

FlowForge is a local-first execution-control platform for AI and automation workloads. It monitors running jobs, applies policy when behavior becomes risky, and records exactly what happened and why.

2) Problem We Solve

- Runaway jobs can burn tokens/API spend quickly.
- Failures can destabilize machines and interrupt operations.
- Most teams lack clear incident evidence and root-cause visibility.
- Trust in autonomous workflows drops when interventions are opaque.

3) Mission and Positioning

Mission: make FlowForge the trusted execution-control reliability layer for AI operations.

- Deterministic execution guardrails
- Explainable policy decisions
- Evidence and audit trail by default
- Reliability discipline as part of product value

Current non-goal: broad multi-tenant SaaS expansion before reliability proof.

4) Product Loop (How it Works)

Run Job -> Observe Signals -> Evaluate Policies -> Act Safely -> Record Evidence -> Improve Rules

5) What We Build Now vs Later

Build Now (P0/P1)	Build Next (After Proof)	Not In Scope (Current 12 Months)
Runtime guard correctness	Cost/model intelligence depth	Multi-tenant hosted SaaS
Decision transparency + versioning	Selective integrations	Billing-first packaging
Policy governance (shadow/canary/enforce)	Enterprise compliance utilities	Black-box auto-remediation
Unified evidence/audit events	Advanced runtime platform layers	Feature expansion without reliability proof
SLO + error-budget rituals	Team-level governance workflows	Broad integrations without design-partner pull

6) Customer and GTM Wedge

Primary user: engineers/operators running long local AI or automation jobs.

First 60-second proof: install works, demo shows intervention and recovery, timeline explains why.

- Local CLI adoption
- Real-workload pilot users
- Evidence-backed retention and trust metrics
- Selective team rollout, then enterprise expansion

7) 12-Week Execution Plan

- Weeks 1-2: reliability foundation
- Weeks 3-4: explainability and evidence quality
- Weeks 5-6: pilot loop and pain-based priorities
- Weeks 7-8: operational maturity (SLO/release/security ritual)
- Weeks 9-12: distribution repeatability

8) 24-Month Roadmap

- Months 0-3: core trust lock
- Months 4-6: operator confidence
- Months 7-12: disciplined expansion
- Months 13-18: platform consolidation
- Months 19-24: enterprise readiness gate

9) Success Metrics

- Time to first value
- Detection latency
- False-positive rate
- Recovery success rate
- CI/reliability gate pass rate
- 7-day pilot retention
- Incident MTTD/MTTR and corrective-action closure rate

10) Business Model Direction

- Core local runtime package
- Team reliability bundle
- Enterprise trust/governance bundle

Commercial principle: monetize trust, reliability, and avoided cost.

11) Non-Negotiable Operating Rules

- No major expansion while reliability gates fail
- No release without rollback readiness
- No feature without metric + rollback path
- No black-box interventions

12) Current Status Snapshot

- In place: strict CI, branch protection, release checkpoint, policy canary, unified event schema
- Near-term gaps: formal weekly SLO dashboard ritual, published chaos drill evidence, external first-time usability validation

External one-line pitch: FlowForge is the local-first execution-control layer for AI workloads that detects risky runtime behavior, intervenes safely, and proves every action with clear evidence.

Source docs: plan.md, docs/COMPANY_EXECUTION.md, docs/RUNBOOK.md, docs/OPERATIONS.md