LAYER 8

Incident Response & Kill-Switch Playbook

Operational Resilience & Deterministic Execution Control

1. Purpose of This Playbook

This playbook defines deterministic operational procedures for incident response within Layer 8 execution governance infrastructure. It ensures controlled failure states and immediate execution containment.

2. Incident Classification

- Billing-Execution mismatch
- Unauthorized execution attempt
- Webhook signature validation failure spike
- Subscription revocation inconsistency
- System abuse or fraud pattern detection
- Infrastructure compromise suspicion

3. Global Kill-Switch Procedure

- Step 1: Activate GLOBAL_KILL_SWITCH flag in KV namespace.
- Step 2: Confirm /access endpoint returns system_paused.
- Step 3: Log activation timestamp and responsible operator.
- Step 4: Notify internal stakeholders and affected clients.
- Step 5: Begin root cause investigation.

4. Revocation Incident Handling

- Verify Stripe event authenticity.
- Confirm subscription status transition.
- Force status = revoked if required.
- Clear entitlements immediately.
- Audit denial logs for attempted post-revocation execution.

5. Trial Expiry Enforcement Validation

- Confirm trial_end timestamp exists.
- Validate current timestamp comparison logic.
- Ensure trial_expired denial response returned.
- Audit access logs for unauthorized post-trial execution.

6. Deterministic Failure Reason Audit

- trial_expired
- revoked
- feature_not_allowed
- inactive_status
- system_paused
- not_found

7. Post-Incident Review Process

- Document timeline of event detection and containment.
- Confirm execution was fail-closed.
- Verify no unauthorized runtime actions occurred.
- Assess need for policy update.
- Produce exportable audit summary for stakeholders.

Prepared by Legal Tech Counsellor — Governance Infrastructure Division