AG Runbook — Phase-4.4 Security Operations

This runbook defines the Security Operations layer for the DMS SaaS platform. It consolidates KPI definitions, dashboard design, SOC2 mappings, and incident escalation workflows into a single autonomous execution unit.

1. Objective

Establish observable, measurable, and auditable security operations without introducing automatic enforcement or tenant risk.

2. Scope

In scope: Security KPIs, dashboards, compliance evidence, incident workflows. Out of scope: automatic remediation, account lockouts, SIEM integrations.

3. Inputs

- Audit logs (append-only, tenant-scoped)
- Security alerts (Phase-4.4 taxonomy)
- Session & MFA lifecycle events
- Tenant isolation middleware
- Admin-only UI framework

4. Deliverables

1. Deterministic SQL & Prisma queries per KPI
2. Security Dashboard UI layout
3. SOC2 control mappings
4. Incident escalation workflows

5. Execution Steps

Step A: Define tenant-safe KPI queries (SQL + Prisma).
Step B: Design admin-only Security Dashboard layout.
Step C: Map KPIs to SOC2 Trust Services Criteria.
Step D: Define human-driven incident escalation workflows.

6. Acceptance Criteria

- All KPIs backed by authoritative queries
- Dashboard supports drill-down to evidence
- SOC2 controls mapped with clear evidence
- Incidents are auditable end-to-end

7. Phase Boundary

Completes Phase-4.4. Enables Phase-5 auto-remediation, SOC2 Type II monitoring, and customer-facing security reporting.

8. Summary

This runbook transforms security signals into operational intelligence, compliance readiness, and structured response without compromising tenant isolation.