Production Deployment Checklist

Before Launch

- Secrets in vault
- Rate limiting
- Retry logic
- Queueing
- Structured logs
- Health checks
- DB pooling
- CI/CD
- Rollback strategy
- Human approval console
- Policy engine live
- Audit logs enabled
- Monitoring dashboards
- Incident runbooks
- MCP servers pinned to a known-good tool-definition hash, with re-approval required on change (New)
- OAuth issuer validation enabled on every MCP client (New)

Revision #1
Created 2026-08-24 12:10:27 UTC by Aisha M. Nur
Updated 2026-08-24 12:10:38 UTC by Aisha M. Nur