Skill: ALPHA Agent Platform

When to use

- Adding or modifying one of the ten ALPHA modules
- Designing an agent, swarm, DAG workflow, or MCP integration to be represented in ALPHA
- Writing documentation or policy for agent behavior, memory, security, or commerce

Capabilities

Capability	Module	Entry point
Fleet overview	Command Center	`components/pages/dashboard-page.tsx`
Mesh topology & node inspection	Agent Mesh	`components/pages/agent-mesh-page.tsx`
Workflow design	DAG Editor	`components/pages/dag-editor-page.tsx`
Agent-to-agent messaging	A2A Comms	`components/pages/a2a-comms-page.tsx`
Collective orchestration	Swarm Manager	`components/pages/swarm-manager-page.tsx`
Tools, APIs, databases	MCP Registry	`components/pages/mcp-registry-page.tsx`
Layered memory	Memory Store	`components/pages/memory-store-page.tsx`
Models, tokens, cost, evals	AgenticOps	`components/pages/agentic-ops-page.tsx`
Detection & remediation	Self-Healing	`components/pages/self-healing-page.tsx`
NL control & agent builder	Assistant Hub	`components/pages/assistant-hub-page.tsx`

Procedure: add a new module

1. Add the section id to `NavSection` in `nextjs_space/lib/types.ts`.
2. Add the sidebar entry in `components/alpha-sidebar.tsx`.

3. Create `components/pages/<name>-page.tsx` wrapped in `PageWrapper`.
4. Register it in `components/alpha-shell.tsx` via `next/dynamic` with `ssr: false`.
5. Add mock data to `lib/mock-data.ts` with explicit types.
6. Update README module table, ARCHITECTURE.md, and CHANGELOG.md.

Procedure: define an agent

Follow the agent card format in AGENTS.md: id, role, capabilities, model, tools (allow-list), memory namespaces, budgets, escalation policy.

Guardrails

- Every loop must declare `maxIterations`, `tokenBudget`, and `timeoutMs`.
- Tools are deny-by-default; list them explicitly per agent.
- Irreversible actions (payments, production changes, outbound messages to humans) require human approval.
- Do not label a security control as active in UI or docs unless it is implemented.

References

ARCHITECTURE.md · AGENTS.md · MEMORY.md · SECURITY.md · docs/AGENTIC_COMMERCE.md