SPEAR ENTERPRISE LLC

AGENT OPERATIONS GUIDELINES

Phase 19 - Phase 22

1. PURPOSE

This document defines procedural guidelines governing the transition from design exploration to full SDK-based autonomous agent execution across Phase 19 through Phase 22. The intent is to maintain strict separation between exploratory Digital Twin work and production engineering outputs, while enabling deterministic, auditable execution.

2. DEFINITIONS

ChatGPT Agents (Digital Twin): Role-based simulated agents used for thought experiments, trade studies, internal workflows, and drafting Decision-to-Execution Packets (DEPs). SDK / AgentKit Agents (Production Swarm): Real agents issued agent IDs, capable of reading and writing files, updating databases, and executing workflows via n8n. NAS: WD EX4100 storage system. Spear MCP Share: The only NAS share authorized for SDK Agent write operations. ChatGPT Work Share: A separate NAS share for manually saved ChatGPT-generated artifacts.

3. NAS SHARE AUTHORIZATION POLICY

SDK Agents may read from the Spear MCP Share and may write only to the Spear MCP Share. They are forbidden from writing to any other NAS share. ChatGPT Agents do not perform autonomous NAS writes. All ChatGPT outputs are manually reviewed and saved to the ChatGPT Work Share.

4. PHASE 19 - NAS VISIBILITY AND DATABASE FOUNDATION

Objective: Establish full visibility of the NAS file universe prior to governance declaration. Activities include building a metadata database via read-only crawl of all NAS shares. No file movement, deletion, or reorganization is permitted during this phase.

5. PHASE 20 - SDK AGENT ARCHITECT INITIALIZATION

Objective: Introduce the SDK Agent Architect with limited authority. The Agent Architect has read-only access to the NAS database and Spear MCP Share, and is responsible for analyzing the file universe and proposing canonical structure and cleanup plans.

6. PHASE 21 - DIGITAL TWIN DESIGN AND DECISION MATURATION

Objective: Finalize design intent using the ChatGPT Digital Twin. ChatGPT Agents explore options, resolve conflicts, and draft DEPs. All outputs remain outside production until manually approved.

7. PHASE 22 - FULL SDK SWARM AUTONOMY

Objective: Enable full autonomous execution by the SDK Agent Swarm. Conditions include completed NAS database, approved canonical structure, active governance workflow, and approved DEPs. SDK Agents write only to the Spear MCP Share.

8. CORE PRINCIPLE

ChatGPT Agents think. SDK Agents do. NAS Canon remembers.

9. END STATE

The Digital Twin continues as a planning layer, the SDK Swarm executes real engineering work, and the Spear MCP Share remains the single system of record.