Chapter 1 — Introduction & Scope

1.1 Document Purpose

This document (LH-SBS-INF-001) is the authoritative infrastructure specification for The Dash — SBS's Multi-Gated AI Orchestrator Platform, designed by Ledger Hub Networks exclusively for SBS. It defines the complete DigitalOcean hosting environment on which the Platform operates: account and project structure, network topology, DNS and domain architecture, TLS and edge security, compute and storage layers, secrets management, identity integration, infrastructure-as-code practice, observability, audit infrastructure, and backup and disaster recovery.

The specification serves four functions. First, it is the build reference: every infrastructure resource provisioned for the Platform must conform to the configurations stated herein, and any deviation requires a documented change under the governance forms in effect for the engagement (LH-SBS-CO- series). Second, it is the verification baseline: the acceptance gates defined in LH-SBS-INST-001 (V1–V22) test the environment against this document. Third, it carries the Build Register (Appendix, Chapter 18): the tracked checklist of provisioning items, security controls, and **open nonconformances between the design target and the as-built state**, with per-item completion status. Fourth, it is the operating reference for the IT execution owner (Nelson Santos, IT Director) and any personnel subsequently authorized to administer the environment.

Where the as-built environment deviates from the design target, this document states **both**: the target configuration (normative) and the current state (informative, dated), with the gap tracked in the Build Register. A statement of current state is not acceptance of it.

This document is 100% technical in content. Commercial terms, fees, and engagement governance are out of scope and are addressed in their respective controlling documents.

1.2 Platform Context

The Dash is a zero-trust, identity-aware platform that runs SBS's routine corporate workflows through isolated, per-function Compartments. Inside each Compartment, three classes of AI agents operate under supervision — Workflow Agents perform the first-pass work, Guardian Agents enforce policy and Risk Tiers, and Supervisor Agents route Medium/High/Critical decisions to named SBS staff. The domain is publicly resolvable but serves a private audience behind SSO and phishing-resistant MFA; every agent decision is written to a tamper-evident, hash-chained audit log.

The Platform is hosted on DigitalOcean under a dedicated SBS account, organized into two DigitalOcean Projects that define the environment topology:

- **SBS The Dash Dev** — development and staging environment
- **SBS The Dash Prod** — production environment

All internal service-to-service traffic is required to remain on private VPC networking. Public exposure is restricted to hardened entry points in two classes.

Tenant surfaces (three-subdomain tenant model):

- `sbsdash.com` — primary tenant surface
- `admin.sbsdash.com` — administrative console
- `clients.sbsdash.com` — client-facing surface

Operational surfaces:

- `monitor.sbsdash.com` — observability stack (Grafana dashboards, Prometheus metrics); deployed and live; access to be IdP-enforced (Chapter 9)
- `wiki.sbsdash.com` — documentation portal (BookStack); hosts platform runbooks, configuration references, and operational procedures

Operational surfaces carry no tenant data and sit behind the same TLS, reverse-proxy, and firewall controls as the tenant surfaces, with access scoped to administrative roles only under the least-privilege model of the IAM control family.

Each of the ten functional Compartments is isolated across eight layers — frontend, authentication, application, data, storage, secrets, network, and audit — and this specification defines how each isolation layer is realized in infrastructure: firewall rule sets and VPC segmentation (network); per-Compartment separation across the PostgreSQL, MongoDB, and Redis data services (data, storage); Vault namespace separation (secrets); and hash-chained log capture (audit). The infrastructure supporting the audit log — its storage, integrity chain, and retention — is specified in Chapter 13.

The environment follows a zero-trust posture per NIST SP 800-207 and application controls aligned to OWASP ASVS L2, with AI-specific controls addressing the OWASP LLM Top 10 (including LLM01 prompt injection) as carried in LH-SBS-SEC-001.

1.3 Referenced Documents

Document ID / Source	Title	Relationship to this Specification
LH-SBS-KO-001 V3.2	Technical Install and Discovery	Master runbook. This specification elaborates the infrastructure control families imported into KO-001 from the Foundation Install Spec (Vault, IaC, supply-chain, observability, backup/DR, hash-chained audit, identity depth, WordPress isolation).

Document ID / Source	Title	Relationship to this Specification
LH-SBS-SEC-001	Security & Access Control Specification	Controlling security baseline. The control families (DNS, TLS, IAM, APP, AI, INF, FE, MON) constrain every configuration stated in this document. The Build Register in Chapter 18 tracks implementation status per control ID. *Control-set reconciliation pending: the Build Register enumerates 41 control IDs against the 36 recorded in SEC-001 V1.0; SEC-001 revision to V1.1 or register correction to follow.*
LH-SBS-PRE-001	Pre-Install Prerequisites	Gate conditions. The nine prerequisite gates must be satisfied before any resource defined in this specification is provisioned (Day 0).
SERVER_CHANGELOG.md	Server Changelog — SBS Infrastructure	Operational as-built log maintained by platform engineering. Feeds the Build Register with dated change entries and verification evidence. Entries in the changelog do not modify this specification; divergences it records are tracked as nonconformances. **The changelog must contain no credentials** (INF-02); see Build Register item 15.

Where this specification and LH-SBS-SEC-001 address the same control, LH-SBS-SEC-001 states the requirement and this document states the implementation. In the event of conflict, LH-SBS-SEC-001 controls and this document shall be corrected.

Revision #4
Created 2026-07-17 23:08:30 UTC by SBS Admin
Updated 2026-07-18 05:06:17 UTC by SBS Admin