NEURALPORT

Information Security Management System (ISMS)

Comprehensive Architectural Blueprint & Compliance Ledger

SYSTEM NAME: Swanson India Portal
COMPANY: Swanson Plastics India Pvt. Ltd.
ENVIRONMENT: Production (Vercel Edge + Cloudflare + Supabase)
VERSION: 5.0
EFFECTIVE DATE: May 30, 2026
DRAFT BY: NeuralPORT Systems & Solutions
CLASSIFICATION: Confidential / Client Release

Table of Contents

1. Introduction & Scope Definition

1.1 Purpose of Document

This document serves as the definitive Information Security Management System (ISMS) Master Ledger for the Swanson India Portal. It provides independent auditors, compliance officers, and executive stakeholders with an exhaustive, transparent view of the systemic controls, logical perimeters, and cryptographic boundaries architected by NeuralPORT Systems & Solutions.

1.2 Boundary & Scope

The scope of this framework covers the entire lifecycle of data processing within the Swanson India Portal. This includes:

- The frontend application layer hosted on the Vercel Edge Network.
- The intermediate API communication and routing layers.
- The identity management and backend PostgreSQL database kernel hosted on Supabase (AWS).
- All internal manufacturing data (Quality Control, Logistics, Production Instructions, and Human Resources).

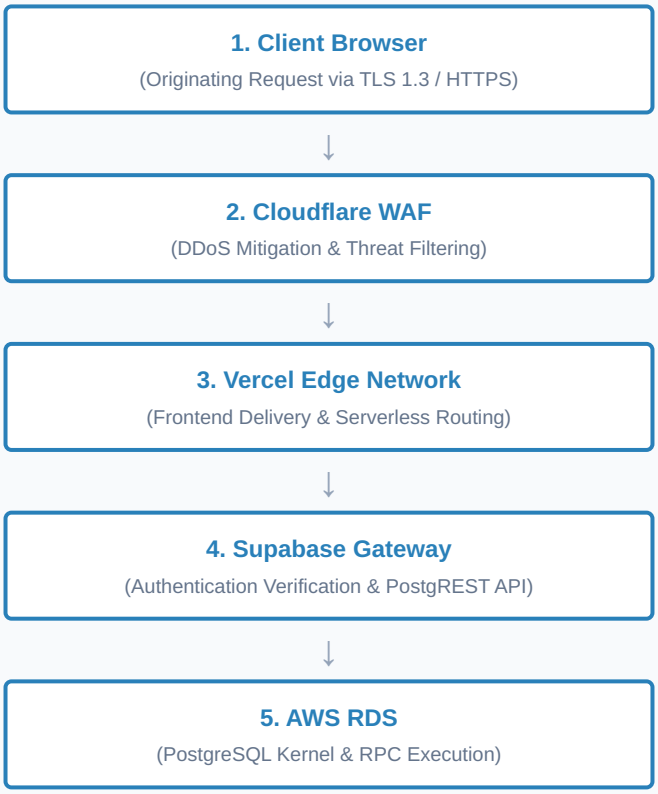
Out of Scope: Physical security of the manufacturing plant, local employee hardware (laptops/scanners), and third-party ISP networks.

2. Infrastructure & Cloud Architecture

2.1 Network Perimeter Defense

The architecture employs a Zero-Trust Edge strategy to neutralize threats before they reach operational logic. Data moves through a strict, vertical gateway protocol designed to aggressively filter malicious payloads.

FIGURE 1: CLOUD INFRASTRUCTURE DATA FLOW



2.2 Provider Compliance Framework

To satisfy rigorous ISO 27001 requirements, the platform utilizes infrastructure providers that undergo continuous, independent third-party attestation.

- **AWS (Amazon Web Services):** Provides the physical datacenter layer. Certified SOC 1/2/3, ISO 27001, ISO 27017, and ISO 27018.
- **Supabase:** Manages the database and identity engine. Holds independent SOC 2 Type II and ISO/IEC 27001:2022 certifications. Real-time audit postures are verifiable at *trust.supabase.io*.

3. Identity & Access Management (IAM)

3.1 Cryptographic Authentication

Access to the Swanson India Portal strictly mandates cryptographic validation. Traditional, plaintext authentication vectors are systematically blocked. Credentials undergo client-side hashing before transmission, and the Supabase Identity Provider utilizes modern computational-heavy hashing algorithms (e.g., bcrypt/Argon2) at the database layer. Successful validation results in the generation of a time-limited JSON Web Token (JWT).

3.2 Session Governance & Lifecycle

Tokens are managed with explicit state control to prevent session hijacking and token replay attacks:

- **Token Isolation:** The architecture strictly forbids the long-term storage of sensitive credentials in vulnerable browser vectors (e.g., standard `localStorage`). Session state is managed via secure, HttpOnly cookie directives or short-lived memory contexts depending on the deployment tier.
- **Revocation Protocols:** Invoking the application "Logout" function triggers a deterministic destruction sequence: the JWT is dropped, browser cache is washed, and active navigation history is overwritten to prevent back-button access to cached DOM elements.

4. Role-Based Access Control (RBAC) Hierarchy

4.1 Multi-Dimensional Access Matrix

Authorization is not binary. The system utilizes a tripartite relational model to calculate explicit user privileges dynamically during every transaction.

FIGURE 2: TRIPARTITE RBAC CALCULATION MATRIX

1. Department Scope

Restricts data visibility to the user's operational silo (e.g., QA, Production, Warehouse).

2. Hierarchical Level

Restricts action types. Level 0 handles data entry. Level 1 handles workflow approvals.

3. Admin Override

A boolean absolute that permits cross-silo auditing and system configuration.

4.2 Workflow Integrity & Separation of Duties (SoD)

Crucial business operations, such as Goods Receipt Note (GRN) approvals, enforce strict Separation of Duties. The architecture dictates that a Quality Control operator cannot programmatically execute a Warehouse Head approval, even if utilizing the same terminal, due to backend cryptographic signature requirements linked directly to the JWT claims.

5. Data Classification & Cryptography Governance

5.1 Internal Data Classification Model

To apply appropriate cryptographic controls, data is classified into three operational tiers:

Classification Tier	Data Types	Handling Protocol
Tier 1: Public/Standard	System UI elements, public document templates, non-sensitive static assets.	Standard edge caching permitted via Vercel CDN.
Tier 2: Internal Operational	Production orders, routing sheets, daily inventory counts.	Requires valid JWT. Cached strictly within authenticated local context.
Tier 3: Confidential	Quality formulations, user credentials, employee PII, systemic audit logs.	Strict database RLS enforced. Zero client-side caching permitted.

5.2 Encryption Standards & Key Management

All data architectures operate under a "Zero-Knowledge Transmission" mandate.

- **Data in Transit:** 100% of network traffic is encapsulated within TLS 1.2 or TLS 1.3 tunnels. Fallback to unencrypted HTTP is administratively disabled at the DNS and WAF layers.
- **Data at Rest:** The underlying disk volumes and snapshot archives are block-encrypted utilizing the Advanced Encryption Standard (AES-256).
- **Key Management:** Infrastructure cryptographic keys are managed automatically by the AWS Key Management Service (KMS), with zero exposure to application-level code.

6. Row Level Security & Database Isolation

6.1 Deterministic Database Security

Frontend UI hiding is deemed insufficient for enterprise security. The Swanson India Portal relies on Row Level Security (RLS) policies embedded directly into the PostgreSQL kernel. If an attacker bypasses the frontend application, the database itself mathematically refuses to return rows that do not match the embedded JWT's claims.

6.2 Secure RPC & Database-Level Logic Execution

To fundamentally mitigate client-side manipulation, critical business logic is abstracted entirely away from the JavaScript frontend. Complex operations, multi-stage approvals, and sensitive state mutations are executed strictly within the PostgreSQL kernel via Remote Procedure Calls (RPCs).

These server-side functions utilize `SECURITY DEFINER` directives. This guarantees that operational workflows execute with strict, predefined database privileges, rather than trusting the invocation context or data payloads provided by the client browser.

6.3 Protected Data Domains

Information Domain	Covered Sub-Systems	RLS Enforcement Protocol
Manufacturing Ops	Material Master, Recipe Configs, Production Orders	Restricted to Production Level 1 & Admin. Write-access isolated to supervisory JWTs.
Document Control	DCN Notices, QMS Documents, Versioning	Read-access globalized for policy adherence; Write-access strictly gated to QA Level 1.
Supply Chain	Stock Master, Supplier Registry, GRN, Dispatch	Cross-departmental conditional access based on specific approval stage logic.
Quality Assurance	Quality Alerts, Floor/Lab Inspections	Creation unrestricted for shift workers; Deletion/ Modification isolated to QA Admins.

7. Endpoint & Client-Side Security Controls

7.1 Cross-Site Scripting (XSS) & Injection Mitigation

To protect the integrity of the client session against injection payloads, the following strict boundaries are maintained:

- **Input Sanitization:** All user-supplied text inputs are aggressively sanitized via client-side libraries prior to transmission, stripping out executable scripts and malformed HTML tags.
- **Query Parameterization:** All backend PostgreSQL queries utilize strict parameterization via the PostgREST API, completely neutralizing SQL Injection vulnerabilities. Direct string concatenation in SQL execution is strictly prohibited.

7.2 Content Security Framework

The application is structured to utilize strict HTTP header controls, instructing the browser engine to reject unauthorized cross-origin resource sharing (CORS) attempts, enforce HTTPS via HSTS, and prevent clickjacking via iframe encapsulation restrictions (X-Frame-Options).

8. Audit, Logging & Incident Response Plan

8.1 Temporal Attribution & Immutability

System-wide non-repudiation is achieved via programmatic database triggers. Every creation and modification event across core operational tables automatically captures standard `created_at` and `updated_at` timestamps. These fields are strictly immutable via standard API pathways, guaranteeing forensic integrity.

8.2 Disaster Recovery & Business Continuity (DR/BC)

The architecture provides robust resilience against data corruption or infrastructure failure:

- **Automated Snapshots:** Full systemic backups are executed automatically on a 24-hour cycle.
- **Point-in-Time Recovery (PITR):** The database engine maintains active Write-Ahead Logging (WAL). In the event of catastrophic logical corruption, the System Architect can restore the database to any specific second within the retention window, resulting in a near-zero Recovery Point Objective (RPO).

8.3 Incident Response Workflow

In the event of an identified security anomaly or data breach, NeuralPORT follows a strict remediation workflow:

1. **Identification & Containment:** Anomalous sessions are immediately terminated via the Supabase Admin Console. WAF rules are aggressively updated to block offending IP ranges.
2. **Forensic Review:** Database logs and PITR archives are reviewed to determine the scope of unauthorized access.
3. **Stakeholder Notification:** Executive leadership at Swanson Plastics India Pvt. Ltd. is notified with an immediate impact assessment and remediation timeline.

9. Secure Software Development Life Cycle (SSDLC)

9.1 AI-Assisted Architecture Controls

NeuralPORT utilizes an advanced, prompt-driven AI development methodology. To ensure generated code meets enterprise security standards, the following SSDLC controls are enforced by the System Architect:

- **Prompt Governance:** All system architectures are generated using strict System Security Prompts that mandate input sanitization, environment variable usage, and strict adherence to the avoidance of plaintext credential hardcoding.
- **Environment Separation:** Credentials, API Keys, and Supabase connection strings are isolated from the codebase and injected via secure Edge configuration variables at runtime, guaranteeing that source code repositories remain fundamentally clean of sensitive material.
- **Code Sanity Reviews:** Structural changes to the database schema or authentication flows undergo independent architectural review prior to production deployment.

10. Compliance & Continuous Improvement Roadmap

> **Auditor Note on Continuous Improvement:**
>
> In alignment with the ISO 27001 Plan-Do-Check-Act (PDCA) cycle, NeuralPORT maintains an active, phased roadmap to continuously elevate systemic security postures as the threat landscape evolves.

10.1 Near-Term Optimization (Phase 1 & 2)

- **Session Architecture Upgrade:** Refactoring persistence layers to utilize cryptographically attested server-side tokens, fully eliminating client-storage reliance.
- **RLS Perimeter Expansion:** Systematic rollout of granular RLS policies to secondary user profile and inspection metrics tables.
- **API Gateway Hardening:** Deployment of programmatic rate-limiting to mitigate brute-force and resource-exhaustion vectors.

10.2 Mature Operations (Phase 3)

- **MFA Deployment:** Integration of Time-Based One-Time Password (TOTP) Multi-Factor Authentication for all administrative and Level 1 supervisory accounts.
- **Unified Audit Ledger:** Creation of an isolated, append-only database ledger strictly for tracking user logins, permission elevations, and data export events.

Independent Infrastructure Attestation

The underlying hardware perimeters, hardware patch state, and infrastructure lifecycle operations maintain rolling independent validations accessible openly via the platform's Trust Gateway:

trust.supabase.io

SOC 2 Type II Certified | ISO/IEC 27001:2022 Verified | GDPR Data Privacy Aligned | PCI DSS Compliant Backing | HIPAA Technical Readiness