DMS SaaS — Security & SOC2 Documentation

Purpose & Scope

This document describes the security guarantees, invariants, and enforcement mechanisms of the DMS SaaS platform. It reflects the implemented system.

Core Security Principles

Tenant isolation is enforced at the database layer post-authentication.
Authentication, authorization, and tenant isolation are separate concerns.
All post-auth access must be tenant-bound.

Authentication & Session Security

JWT access tokens with rotating refresh tokens.
Refresh tokens represent sessions and can be revoked individually or globally.

PRE_AUTH vs POST_AUTH

PRE_AUTH allows limited identity resolution without tenantId.
POST_AUTH requires tenantId for all database access.

Tenant Isolation Enforcement

Implemented via Prisma middleware with logging-first strategy.
Models classified as TENANT_SCOPED, TENANT_RELATED, USER_SCOPED, GLOBAL.

Authorization Model

RBAC with permissions and roles.
Authorization does not bypass tenant isolation.

Security Alerts

Security-relevant actions generate tenant-bound alerts.

Final Invariant

Tenant isolation is enforced at the DB layer post-auth, relaxed only for identity resolution pre-auth.