DMS SaaS — Security and SOC 2 Control Documentation

0. Purpose and Scope

This document formally describes the security architecture, control objectives, and enforcement mechanisms implemented within the DMS SaaS platform. The intent of this documentation is to provide auditors, security reviewers, and internal stakeholders with a clear and accurate representation of the system's security posture. All statements herein reflect the system as implemented in production and are not aspirational.

1. Core Security Principles

The DMS SaaS platform is designed around explicit security boundaries. The following principles are considered non-negotiable and apply to all current and future system components.

1.1 Tenant Isolation as a Hard Boundary

Data belonging to one tenant is strictly isolated from all other tenants. Tenant isolation is enforced at the database access layer and does not rely on application routing, user interface controls, or client-side logic.

1.2 Separation of Security Concerns

Authentication, authorization, and tenant isolation are treated as independent concerns. Authentication establishes identity, authorization determines permitted actions, and tenant isolation constrains the data scope. A failure or bypass in one layer does not compromise the others.

1.3 Post-Authentication Tenant Binding

Once authentication has succeeded, all subsequent data access operations are required to be tenant-bound. Any post-authentication database operation that is not explicitly scoped to a tenant is classified as a security defect.

2. Authentication and Session Security

The platform uses a token-based authentication model designed to minimize session persistence risk while providing strong guarantees around session invalidation.

2.1 Token Architecture

Short-lived JSON Web Tokens (JWTs) are used for access authentication. Long-lived refresh tokens are rotated on each use and stored server-side. Compromise of an access token does not permit long-term access.

2.2 Session Representation

Each refresh token represents a single logical session. Sessions are associated with metadata such as device identifier, IP address, and last activity timestamp.

2.3 Session Revocation Guarantees

Users and administrators may revoke individual sessions or all sessions except the current one. Upon revocation, the associated refresh token becomes immediately unusable. Revoked sessions cannot be reinstated.

3. Pre-Authentication and Post-Authentication Boundary

The system explicitly differentiates between pre-authentication and post-authentication request handling. This distinction is critical to maintaining secure tenant isolation.

3.1 Pre-Authentication (Identity Resolution)

Pre-authentication flows include login and password recovery processes. During this phase, a tenant identifier may not yet be known. Limited user lookup operations are permitted solely for identity resolution and are constrained to specific fields.

3.2 Post-Authentication (Tenant-Enforced Operations)

All authenticated requests operate within a trusted tenant context derived from cryptographically verified tokens. All database access during this phase must include tenant scoping. Violations are treated as high-severity findings.

4. Tenant Isolation Enforcement Mechanism

Tenant isolation is enforced through centralized database middleware. This approach ensures uniform application across all query paths and prevents accidental bypass.

4.1 Model Classification

Data models are explicitly classified as tenant-scoped, tenant-related, user-scoped, or global. Each classification has defined enforcement requirements that are reviewed during development.

4.2 Logging-First Enforcement Strategy

The system currently operates in a logging-only enforcement mode. This mode records violations without blocking execution, allowing real-world detection of cross-tenant access risks prior to full enforcement.

5. Authorization Model

The platform employs a role-based access control (RBAC) model. Permissions are atomic and assigned to roles. Users are assigned roles within a tenant context. Authorization checks do not bypass tenant isolation constraints.

6. Security Alerts and Audit Signals

Security-relevant events, including session revocation and password changes, generate immutable security alerts. All alerts are tenant-bound and attributable to a specific user and event source.

7. Explicit Non-Goals and Risk Reductions

The system intentionally avoids implicit tenant inference, database access within authentication guards, and reliance on client-side enforcement. These exclusions are deliberate risk-reduction measures.

8. Forward Enforcement Plan

The platform supports future transition to selective and full enforcement modes. Enforcement will be introduced incrementally with monitoring, feature flags, and rollback mechanisms.

9. Authoritative Security Invariant

Tenant isolation is enforced at the database layer following authentication and is intentionally relaxed only for controlled identity resolution prior to authentication.