SOC 2 Type II Control Coverage — DMS SaaS

CC1–Control Environment

Defined security responsibilities, RBAC enforcement, and administrative separation operate consistently.

CC2–Communication

Security responsibilities and access rules are documented and enforced across teams.

CC3–Risk Assessment

Tenant isolation and auth boundaries are reviewed and monitored in production.

CC4–Monitoring

Security alerts and logs operate continuously and are reviewed.

CC5–Control Activities

Automated tenant enforcement middleware operates on every DB query.

CC6–Logical Access

Authentication, authorization, and tenant isolation controls operate as designed.

CC7–System Operations

Session revocation and alerting demonstrate operational effectiveness.

CC8–Change Management

Security-sensitive changes are controlled and observable.

CC9–Risk Mitigation

Kill-switches and enforcement modes reduce blast radius.