Architecture Decision Record (ADR■0001)

WorshipOS — Tenancy & Architecture Promises

Status: Accepted
Date: 2025■12■16
Decision Owners: WorshipOS Core Architecture

Context

WorshipOS is a multi■tenant SaaS system designed for churches. Early architectural decisions established a need for strong data isolation, clear domain language, and long■term safety against cross■tenant data leakage.

Decision

We define the following architecture promises as invariants. Any implementation that violates these promises is incorrect by definition.

Tenant Boundary

A church is the hard isolation boundary. All tenant■owned data must include `church_id`. No query may read or mutate data across church boundaries.

Authorization vs Isolation

`church_id` enforces isolation. `campus_id` is a visibility and authorization scope only. Authorization never substitutes for isolation.

Defense in Depth

Tenant keys are intentionally duplicated across tables to prevent unsafe joins and to make isolation failures obvious.

Views & API Contracts

Views must truthfully expose domain semantics. The API and database use a single, consistent vocabulary. Legacy terms are fully removed.

Migration Authority

The database schema evolves only through migrations. Ad■hoc changes are forbidden.

Consequences

This decision increases schema verbosity and requires more disciplined migrations, but it dramatically reduces security risk and long■term maintenance cost.

Non■Goals / Explicitly Out of Scope

- We will not support cross■church shared data.
- We will not allow campus■level isolation to substitute for tenant isolation.
- We will not support multiple tenant vocabularies (e.g. org_id vs church_id).
- We will not hot■patch production schemas outside migrations.
- We will not optimize prematurely at the cost of clarity or safety.

North Star Test

If two churches run identical data and workflows, neither must be able to observe the other in any way.