Reformeer

Security Report

INGEDIEN DEUR

Reformeer

DATUM

16 Februarie 2026

Reformeer Security Architecture & Data Privacy Report

Executive Summary

This document outlines the security measures protecting the Reformeer platform. Our architecture is built on a **"Zero Trust"** philosophy: no user, device, or request is trusted by default. Every single request for data is strictly verified for identity, authority, and context before any information is retrieved or displayed.

1. The Data Vault (Database Lockdown)

Our database operates as a **secure vault**, completely isolated from direct public access.

- **The Rule:** The database is permanently locked to the outside world.
- **The Reality:** No web browser, mobile application, or external script can directly query the database. Even if the application code were inspected, no access keys would be found, as these are securely managed server-side.
- **The Mechanism:** All data requests must pass through our secure API. This programmatic "checkpoint" verifies credentials and permissions before retrieving any data from the vault.

2. Strict Identity Verification

Before any data is accessed, the requester must definitively prove their identity.

- **Digital Passports:** We utilize enterprise-grade authentication to issue secure, temporary session tokens.
- **Continuous Checks:** Every time the application requests data—from a profile picture to a sensitive pastoral note—this token is verified. If the token is expired, invalid, or missing,

the request is instantly denied.

3. Clear Access Rules (Role-Based Access Control)

Proving identity is only the first step; the system then verifies *authority*. We enforce strictly defined roles to ensure users only see what they are explicitly permitted to see:

A. General Application Access

Access is heavily siloed. A regular member cannot access, for example, the Admin Portal (`Kantoor`) or the Finance System (`Finance`) unless they are given access by a church admin via the Admin Portal.

B. Sinode & Council Documents

Official documents are protected with the highest level of scrutiny.

- **Council Isolation:** Documents belonging to a specific Council are strictly locked to that Council's digital environment.
- **Safe Retrieval:** When a user requests a document, the system performs a real-time check to guarantee the document belongs to their authorized context. Access is granted exclusively for the specific file requested, actively preventing bulk-download attempts.

C. Pastoral & Ministry Notes (Strict Privacy)

Highly sensitive information, such as pastoral notes, mimics strict ecclesiastical workflows:

- **The Pastor View:** Pastors have oversight of their entire Council/flock.
- **The Elder/Deacon View:** An Elder or Deacon can *only* see notes for the specific families assigned to their care (their Wyk). They are entirely blocked from viewing notes regarding members in other wards.
- **The Member View:** Regular members can never view official ministry notes. They are restricted to viewing and managing only their own personal profile data.
- **Author Accountability:** Authors always retain view access to the notes they have written.

4. Strict Church-to-Church Data Isolation

Reformeer enforces strict database boundaries between individual churches. **There is absolutely no "data sharing" or cross-pollination of records between congregations.**

- **Data Remains Localized:** A member's profile, history, and associated pastoral notes cannot "move as is" to another church. All historical data remains securely within the original church's database and is subject solely to that specific church's data retention and deletion policies.
- **The Migration Process:** If a member moves to a new church using the Reformeer platform, their historical data is left behind. Only their fundamental identity data (Name and Email) is migrated. This initiates the creation of a completely **"NEW"** profile within the destination church's isolated database.

5. The Checkpoint (API Security Logic)

All traffic flows through a central API checkpoint. This API checks the user's permissions before retrieving data form the vault, preventing unauthorised access.

6. Legal, Privacy & Compliance

For comprehensive information regarding our data handling procedures, privacy policies, and terms of service, please review our official documentation.

- **View Full Security & Privacy Terms:** reformeer.org/terms