🔐 ReAlign MVP – Security & Privacy Plan

Version: 1.3

Date: May 21, 2025

Goal: Ensure that all user data—especially sensitive financial and legal documents—is protected by default.

## **🔑 Authentication & Session Security**

* **Provider:** Supabase Auth
* **Negotiators:** Email + password login
* **Other roles (homeowners, agents, escrow):** Magic link authentication
* **Magic Link Expiry:** Single use, 24-hour TTL, max 3 resends per hour
* **Sessions:** Supabase handles secure token issuance and refresh
* **Session Storage:** Stored in secure cookies (httpOnly, sameSite=strict)

## **👥 Role-Based Access Control (RBAC)**

* Each user scoped to their transactions via backend middleware
* Middleware checks role + transaction membership
* Only users invited to a transaction can:  
  + View messages
  + Upload documents
  + See their own status
* Negotiators can:  
  + See all data in the file
  + Manage document requests, messages, and phase

## **📁 Document & File Security**

* **Storage:** Supabase Storage with signed URL access
* **Upload Controls:**
  + Users can only upload to transactions they are invited to
  + visibility field controls access: shared vs private
  + Private = negotiator-only
* **Transport:** All file uploads encrypted in transit via HTTPS
* **Download Access:** Signed URLs expire after 5 minutes

## **🧾 Message & Metadata Privacy**

* Messages are flat and scoped to transaction participants only
* Message replies (replyTo) do not expose thread if user doesn’t have access
* No personally identifying information is shown across roles (e.g., buyers cannot see seller email)

## **🧠 Backend & Infrastructure Security**

* **Platform:** Node.js + Express
* **Error Handling:** Centralized middleware to avoid stack traces leaking
* **Logging:** Basic event logs + future audit logs table
* **Rate Limiting:** Auth endpoints throttled (login, magic link, resend)
* **Validation:** Zod used server-side to sanitize all incoming data
* **ORM:** Drizzle with parameterized queries (SQL injection safe)

## **📜 Compliance Considerations**

* No PII or financial documents are shared across users
* Magic links meet MFA-lite standards for short-term access
* Logs and user actions auditable post-MVP

✅ This plan ensures:

* Minimum necessary access by default
* No shared documents unless explicitly allowed
* Signed URLs, role validation, and expiration logic secure all sensitive flows
* Ready for implementation and scaling