G Vision — Security & Privacy

Operational Intelligence for Hotels & Resorts · Prepared for General Managers & IT · April 2026

WHERE YOUR DATA LIVES

- **Hosting:** Vercel (SOC 2 Type II, ISO 27001).
- **Database:** Supabase, Sydney (AU) region. Data stays in Australia.
- **Email:** Resend with SPF, DKIM, DMARC on gvision.app.
- **Encryption:** AES-256 at rest · TLS 1.2+ in transit · Let's Encrypt auto-renewal.

HOW USERS SIGN IN

- Email + password with bcrypt-hashed storage.
- 4-digit department PIN (bcrypt) for floor staff.
- **Two-factor auth** (TOTP) supported with backup codes.
- 8-hour session timeout, 15-minute rolling refresh.
- Cookies: __**Secure-**, HttpOnly, SameSite=Lax (HTTPS-only).
- HMAC-SHA256 signed invite / reset links — immune to email pre-scan.

WHO CAN SEE WHAT

- Multi-tenant isolation by property, enforced at 3 layers:
- 1. Postgres Row-Level Security policies.
- 2. Middleware cross-tenant guard.
- 3. Role-based UI gating.
- Role hierarchy: Super Admin → GM → Resort DM → Manager → Dept Head → Staff → Read-Only.
- Users cannot assign a role higher than their own.

PROTECTION AGAINST ATTACKS

- HSTS (2-year), nosniff, X-Frame-Options, Referrer-Policy, Permissions-Policy.
- X-Powered-By stripped · no production source maps.
- Rate-limiting on MFA, reset, invite, public endpoints.
- Zod validation on every API input.
- Generic error responses — no DB-detail leakage.
- Upload checks (MIME, extension, 10 MB cap) on Excel imports.
- Audit log: every invite, role change, delete, password set.
- Dependabot + npm audit block releases on high/critical vulns.
- ESLint security rules wired into the codebase.

COMPLIANCE

- **Australian Privacy Act 1988** — APP-aligned, AU data residency.
- **GDPR** — subject access & erasure supported; DPA on request.
- Sub-processor DPAs (Vercel, Supabase, Resend) with SCCs.
- No payment card data stored.

WHAT YOU CONTROL

- Export, view and delete any record in your property.
- Instant staff removal (auth + profile cascade).
- Re-invite a deleted email (reclaim flow).
- Full CSV export for compensation, incidents, handover.

Contact: gaelittahpro@gmail.com · **Security disclosure:** https://gvision.app/.well-known/security.txt