ASCENDA

DOWNLOADABLE RESOURCE

Website Security Checklist — 20 points

The list we use internally before calling any site launched. Print it, go through it point by point, and check every box before saying "okay, it's live."

> If your site is a static landing page with no backend, the "Authentication & Data Access" block doesn't apply yet — but go through the rest anyway. The moment you add a form with a database, a login, or a public webhook, the full list comes into play.

SECRETS & KEYS

- [ ] Hide API keys — never hardcoded in the frontend or the repo
- [ ] Remove secrets from Git — check the history, rotate any key that leaked
- [ ] Public vs. private database keys — only the "anon/public" key goes in the client (e.g. Supabase/Firebase); the "service_role"/secret key never leaves the backend

AUTHENTICATION & DATA ACCESS

- [ ] Row-Level Security (RLS) enabled on the database, not just frontend checks
- [ ] Encrypt sensitive data (HTTPS in transit, encryption at rest where it applies)
- [ ] Authentication enforced server-side on every protected endpoint/route, not just a hidden button
- [ ] Record access restricted by owner/tenant — a user should never be able to request someone else's ID
- [ ] Block field/mass-assignment tampering — the client shouldn't be able to set role/price/admin via payload
- [ ] Cookies with HttpOnly, Secure, SameSite flags
- [ ] Passwords hashed (bcrypt/argon2), never stored in plain text or with reversible encryption
- [ ] Login attempt limits (rate-limiting / lockout after repeated failures)

INPUT & CONTENT

- [ ] Always use parameterized queries (never concatenate SQL)
- [ ] Validate every input server-side — don't rely on frontend validation alone
- [ ] Escape user-generated content before rendering it (prevents XSS)
- [ ] Restrict file uploads (type, size, no executables, served without execute permission)

NETWORK & ABUSE

- [ ] Anti-bot protection on public forms (captcha/rate-limit)
- [ ] Rate-limiting / quotas on any public API
- [ ] Security headers: CSP, X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security, Referrer-Policy
- [ ] Force HTTPS everywhere (redirect + HSTS)