# Secure Development Standard

**Voll Studios Ltd (trading as TPSClear), August 2026. Applies to all changes to production systems; adopted by the director and binding on any future developer from their first commit.**

## 1. Principles

All development follows current secure-development practice, OWASP-aligned, with controls enforced by tooling wherever possible so they cannot be skipped under time pressure.

## 2. The standard

### Input handling

- Every external input is validated server-side: type checks, length limits, allowlists. Request bodies are size-capped; batch inputs are count-capped.
- Database access uses parameterised queries via the data client; no SQL built by string concatenation.

### Secrets and least privilege

- Secrets exist only in the platform's encrypted environment configuration, never in source control (enforced by gitignore patterns and repository history checks).
- Services use per-provider scoped credentials; production database access is server-side only, behind a scoped service key, with row-level security enabled.
- Preview and development builds receive no production secrets: production data access is scoped to the production environment only.

### Dependencies

- Production dependencies are kept patched. The verification pipeline fails on high or critical advisories in production dependencies, and the deploy pipeline enforces the same gate, so a vulnerable dependency cannot reach production.

### Change quality gates

- Every change passes strict TypeScript type checking and the automated test suite before deployment.
- All changes are reviewed by the accountable owner before reaching production. There is no separate peer-review team; this is stated plainly rather than claimed otherwise, and compensated by the automated gates above.

### Data handling in development

- Customer data is never used in development or testing; test fixtures are synthetic. AI-assisted development tooling operates on source code only, never on customer data.

**Failure design**

- Security-relevant failures fail closed: a screening provider failure returns Unknown, never Clean; missing configuration returns an error, never a bypass.

## 3. Keeping current

The OWASP Top Ten and platform security guidance are reviewed annually under the security awareness routine, and the standard is updated when the architecture changes. Any future developer acknowledges this standard at onboarding.