Security Posture & Application Security Plan

Asset: kiranregmi.com
Owner: Kiran Regmi

Purpose & Scope

This document outlines the security strategy used to protect kiranregmi.com, focusing on access control, application security, monitoring, and continuous improvement. Security is treated as an ongoing responsibility aligned with professional standards.

Implemented Security Controls

- Authenticated access to protected dashboard features
- Session-based access control and role separation
- Input validation and controlled backend data access
- HTTPS enforced across the application
- Secrets managed via environment variables
- Version-controlled source code with no exposed credentials

Internal Security Review (Gap Assessment)

- Authentication hardening (rate limiting and abuse prevention)
- Bot protection for login and sensitive endpoints
- Security header enforcement (CSP, HSTS, clickjacking protection)
- Centralized monitoring and alerting
- Formalized backup and recovery procedures

Risk-Based Prioritization

Security improvements are prioritized based on likelihood, potential impact, remediation effort, and effect on usability. This ensures practical and effective risk reduction.

Continuous Improvement Plan

- Phase 1: Identity hardening, rate limiting, password policy enforcement
- Phase 2: Monitoring, alerting, and backup automation
- Phase 3: Security maturity improvements and automation

Security Ownership Statement

As the platform owner, security responsibility extends beyond development. Controls, reviews, and improvement plans are maintained to ensure long-term trust, availability, and resilience.