# Application Security Plan

Asset: kiranregmi.com
Owner: Kiran Regmi

## 1. Purpose & Scope

This document defines the security strategy for kiranregmi.com. Security is treated as an ongoing responsibility supporting availability, integrity, and trust.

## 2. Asset Identification

Critical assets include application availability, authentication systems, learning content, user data, source code, and brand reputation.

## 3. Threat Model

Primary threats include credential abuse, automated attacks, web vulnerabilities, misconfiguration, dependency risk, and reputational harm.

## 4. Security Objectives

Prevent unauthorized access, reduce attack surface, detect misuse early, enable rapid recovery, and maintain platform trust.

## 5. Security Architecture

Layered controls are implemented across identity, application, infrastructure, monitoring, and recovery.

## 6. Identity & Access Management

Role-based access control, session management, and least-privilege principles protect authenticated platform features.

## 7. Application Security Controls

Input validation, backend-controlled data access, secure error handling, and minimized endpoints protect the application layer.

## 8. Infrastructure & Hosting Security

HTTPS enforcement, managed hosting, protected environment variables, and restricted administrative access reduce infrastructure risk.

## 9. Monitoring & Logging

Authentication events and anomalous activity are logged to support detection and investigation.

## 10. Incident Response

Incidents follow identification, containment, investigation, recovery, and lessons-learned phases.

## 11. Backup & Recovery

Source-controlled recovery and data backups support rapid restoration of service.

## 12. Governance & Maintenance

Controls are reviewed periodically and after significant changes to ensure effectiveness.

## 13. Continuous Improvement

Security maturity is increased incrementally through prioritized remediation efforts.