Rules of Engagement (RoE)

Independent Security Audit — Rules of Engagement

Auditor: Anuj Panthi
Email: anujpanthi66@gmail.com
Portfolio: anujpanthi.com.np
Contact: 9765875727

Purpose
This Rules of Engagement document defines the authorized boundaries, allowed activities, and operational expectations for the independent 30-day external security audit of Resunga Multiple Campus.

Scope of Testing (Allowed)

- OSINT and public information gathering
- Subdomain enumeration
- DNS and WHOIS analysis
- Non-intrusive port/service scanning
- SSL/TLS configuration review
- Security header evaluation
- Technology fingerprinting
- Non-destructive SQLi, XSS, CSRF testing
- Authentication/session behavior review
- Input/output validation checks
- Public endpoint access control review
- Directory & file exposure evaluation
- Email security checks (SPF, DKIM, DMARC)
- CVSS-based risk scoring

Prohibited Actions

- Exploitation of vulnerabilities
- Backend/database access
- Password cracking
- Payload uploads

- DDoS or stress testing
- Social engineering
- Any intrusive or unauthorized activities

Testing Window
All work will take place within the approved 30-day assessment period.

Data Handling
All collected data will remain confidential and used solely for the purposes of this assessment.
A redacted, non-sensitive version of the final report may later be published on the auditor's portfolio (anujpanthi.com.np) with full credit to the auditor.

Communication
Critical issues will be reported immediately to the designated representative.

Reporting
A final written report will be delivered at the conclusion of the audit.