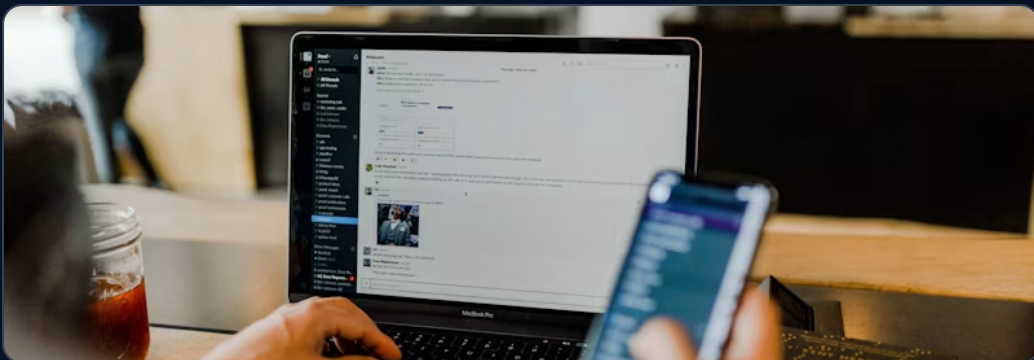




Security & Compliance Guide

Building Secure, Reliable & Trusted Digital Solutions



Enterprise Governance Whitepaper • 2026 Edition

<https://voxorasolutions.in>



Introduction

Security is a fundamental part of every solution we develop at Voxora Solutions. We follow industry best practices to protect applications, user data, and business operations throughout the software lifecycle.

This guide provides an overview of our security measures and compliance-ready development practices designed to maintain data privacy and system resilience.

Our Security Principles



Core Architectural Principles

-  **Security by Design:** Security considerations built into requirements and architecture from day one.
-  **Privacy by Default:** Data minimization and default restrictive permissions.
-  **Least Privilege Access:** User roles limited strictly to necessary functions.



Operational Governance

-  **Defense in Depth:** Multi-layered security controls across networks, servers, and code.
-  **Continuous Monitoring:** Real-time logging and performance tracking.
-  **Secure Coding:** OWASP-aligned development guidelines.



Authentication & Access Control



Authentication Methods

- Email & Password Hashing
- Multi-Factor Authentication (MFA)
- OAuth 2.0 Identity Protocol
- Single Sign-On (SSO)
- Password Reset Token Protection



Access Control

- Role-Based Access Control (RBAC)
- Granular User Permissions
- Admin Access Management
- Secure Session Timeout Controls
- Account Lockout Brute-Force Guards



1. User Requests Login Payload



2. Server Validates Credentials & MFA Token



3. Issued Signed JWT Token with Granular RBAC Permissions



Data Protection & Encryption



In Transit: HTTPS with TLS 1.2 / TLS 1.3 encryption



Password Security: bcrypt & Argon2 hashing



At Rest: AES-256 database storage encryption



Secrets: Encrypted environment variable isolation



Application Threat Protection

Our software engineering safeguards applications against the OWASP Top 10 vulnerabilities:



Protection Against

- ✖ SQL Injection Attacks
- ✖ Cross-Site Scripting (XSS)
- ✖ Cross-Site Request Forgery (CSRF)
- ✖ Clickjacking Vulnerabilities



Attack Mitigation

- ✖ Brute-Force Password Attempts
- ✖ Session Hijacking Attempts
- ✖ Malicious File Upload Exploits
- ✖ API Abuse & Resource Exhaustion



API Security Architecture



Signed JWT API Token Validation



Encrypted API Key Authorization



Dynamic API Rate Limiting & Throttling



Input Data Validation & Schema Binding



Output Sanitization



Real-time API Request Audit Logging



Infrastructure Security

Supported Cloud Platforms: **Amazon Web Services (AWS)** • **Microsoft Azure** • **Google Cloud** • **Linux VPS**



Cloud Hardening

- ✓ Secure Cloud Configuration Isolation
-  Web Application Firewall (WAF) Rules
-  Virtual Private Cloud (VPC) Subnet Isolation



Network Resilience

-  DDoS Protection Layer (Provider Native)
-  Load Balancing & Failover Nodes
-  Automatic OS & Security Updates

Backup & Disaster Recovery



Backup Strategy

-  Automated Daily Off-site Backups
-  Point-in-time Database Snapshots
-  Encrypted Backup Vault Storage
-  Periodic Recovery Testing Routine



Recovery Objectives

-  Minimal Downtime SLA
-  Fast System & Data Restoration
-  Complete Data Integrity Validation
-  Continuous Business Plan Support

Secure Software Development Lifecycle (SSDLC)



Security Testing & Monitoring

 **Pre-Release Testing**

- ✓ Automated Vulnerability Assessments
- ✓ Penetration & Security Testing
- ✓ Authentication & RBAC Boundary Audits

 **Runtime Logging & Metrics**

- ✓ Centralized Error & Exception Logging
- ✓ Immutable User & Admin Audit Logs
- ✓ Real-time API Usage & Anomaly Tracking



Compliance-Ready Architecture

Our engineering frameworks support integration with global regulatory standards:

 GDPR-Ready Development

 HIPAA-Ready Architecture

 PCI DSS Best Practices

 ISO 27001 Aligned Security

 OWASP Top 10 Guidelines

**Note: Full regulatory certification depends on the client's deployment infrastructure, operational policies, and regulatory scope.*

Shared Responsibility Model

Security is most effective as a shared commitment between engineering and business operations. We recommend that clients maintain the following operational habits:

 Enforce strong password policies

 Mandate Multi-Factor Authentication (MFA)

 Periodically review user access privileges

 Keep client endpoint software updated

 Protect API credentials and private keys

 Promptly report suspicious account activity



Why Security Matters

Protect customer data • Build user trust • Mitigate risks • Maintain business continuity • Meet compliance goals

Partner With Voxora Solutions

Security-First Software Engineering



Website: www.voxorasolutions.in



Email: hello@voxorasolutions.in



Phone: +91 70577 66762



HQ: Vasai, Maharashtra, India



Scan to visit www.voxorasolutions.in