ZERO-TRUST ARCHITECTURE & SECURITY CONTROLS

Enterprise Single-Tenant VPC Isolation • Kernel RLS Isolation • Cryptographic Ingestion

TARGET: **Enterprise Evaluation**
SOC 2 Type II & ISO 27001 Aligned

PERIMETER & NETWORK VPC

Single-tenant isolated cloud VPC (AWS Mumbai ap-south-1 & Frankfurt eu-central-1). Ingress restricted strictly to TLS 1.3 endpoints with AWS Shield DDoS mitigation and AWS WAF rate-limiting rules.

`AWS PrivateLink • Isolated CIDR /28`

CRYPTOGRAPHIC TOKEN ENGINE

Referral share links use ephemeral HMAC-SHA256 authenticated query tokens (`?ref=uuid`). Anti-tamper signatures prevent URL parameter tampering, referral hijacking, or unauthorized reward attribution.

`AES-128-CBC Fernet • HMAC-SHA256`

KERNEL ROW-LEVEL SECURITY

PostgreSQL kernel-level Row-Level Security (RLS) guarantees complete cross-tenant boundary isolation. Queries are cryptographically bound to current session tenant IDs at runtime, preventing data crossover.

`Postgres RLS • Zero-Leakage Policy`

NON-ROOT SERVICE EXECUTION

Container workloads operate strictly under unprivileged Linux user contexts (`USER appuser:1001`) with read-only root filesystems and dropped Linux capabilities, eliminating container escape vectors.

`UID 1001 • Read-Only Root FS`

CORE SECURITY & INFRASTRUCTURE PARAMETERS

CONTROL CATEGORY	VOUCHIR PRODUCTION STANDARD	ENTERPRISE VERIFICATION BENEFIT
Authentication (SSO)	SAML 2.0 / OIDC (Okta, Entra ID, Ping)	Centralized IT deprovisioning & enterprise MFA enforcement
Data at Rest & In Transit	AES-256 KMS Customer Keys & TLS 1.3	End-to-end data cipher isolation with forward secrecy
Data Sovereignty & Residency	AWS Mumbai (ap-south-1) / Frankfurt	Guaranteed statutory compliance with Indian DPDP Act & EU GDPR
ATS Ingress & Webhooks	Signed Secret HMAC Webhook Verification	Eliminates candidate spoofing from unauthorized endpoints
Audit Logging & SIEM	Immutable Append-Only Log Stream	Full forensic visibility with export to Datadog, Splunk, or Sumo

Notice: This technical security specification forms part of the enterprise onboarding pack. Dedicated SOC 2 Type II audit reports, ISO 27001 certifications, and third-party penetration test attestations are available upon mutual NDA.

DATA PROCESSING ADDENDUM (DPA)

Statutory Data Fiduciary & Data Processor Boundary Agreement

EFFECTIVE: MASTER SERVICES AGREEMENT

DATA FIDUCIARY (EMPLOYER)

Controls purpose, retention, and means of candidate processing.

- Retains exclusive legal ownership of all candidate CVs, profiles, and hiring notes.
- Defines automated retention schedules (30, 90, or 180-day automated purging).
- Authorizes third-party ATS integrations (Workday, Greenhouse, Lever, Darwinbox).
- Validates candidate legitimate interest and statutory employee advocacy rules.

DATA PROCESSOR (VOUCHIR)

Transient technical intake and referral attribution execution.

- Zero secondary data usage: Candidate CVs are never used to train commercial AI models.
- Zero third-party trackers, marketing cookies, or data-broker syndication rails.
- Sub-processors restricted strictly to Tier-1 infrastructure (AWS KMS, SendGrid, Postmark).
- Enforces automated cryptographic erasure upon candidate Right-to-be-Forgotten notice.

MANDATORY STATUTORY SAFEGUARDS & PRIVACY COMMITMENTS

- ✓ **Candidate Explicit Consent:** Intake forms require active candidate opt-in confirmation before resume indexing or recruiter visibility.
- ✓ **Automated Purge & Right to Be Forgotten:** Automated API endpoint executes cryptographic erasure across active databases and backup snapshots.
- ✓ **72-Hour Statutory Incident SLA:** Contractual commitment to notify the Client DPO within 72 hours of any confirmed security or data incident.
- ✓ **Sovereign Cloud Isolation:** Indian enterprise data resides in AWS ap-south-1 (Mumbai); EU data resides in eu-central-1 (Frankfurt).

FOR THE DATA FIDUCIARY (CLIENT)

Authorized Signatory / DPO Name: _____

Title & Date: _____

FOR VOUCHIR TECHNOLOGIES PVT LTD

Authorized Compliance Officer: _____

Title & Date: Head of Legal & Information Security