VISACHIEF .com

GLOBAL VISA & IMMIGRATION INFRASTRUCTURE

Security & Data Protection Dossier

Government & Public-Sector Edition

A complete account of how VisaChief.com protects identity documents, biometric-adjacent records, and sensitive personal information across its AI-native visa and migration platform — covering sovereignty, zero-trust architecture, post-quantum-ready cryptography, AI assurance, and the control mappings that public-sector procurement requires.

Prepared for government and public-sector evaluation · Not for public release

Rev 1.0 · 25 July 2026

FRONT MATTER

Document Control & Contents

Field	Detail
Document title	VisaChief.com — Security & Data Protection Dossier (Government Edition)
Revision	1.0
Issue date	25 July 2026
Owner	Chief Technology Officer, VisaChief.com
Approver	Executive Leadership Team
Review cycle	Six-monthly, or on material change to architecture, law, or threat environment
Classification	OFFICIAL — Sensitive (Commercial-in-Confidence)
Distribution	Named public-sector evaluators, procurement officers and their advisers
Audience	Security assessors, privacy officers, CISOs, procurement and legal reviewers

Contents

SECTION 1

Executive Summary

VisaChief.com operates a visa and immigration platform that handles some of the most sensitive personal information a citizen will ever surrender: passports and travel documents, national identity numbers, biometric photographs, health and character declarations, financial evidence, family relationships and migration history. We treat that data as the crown jewels it is.

This dossier sets out, without marketing abstraction, the technical and organisational measures that protect it. It is written for assessors: every control is stated in terms that can be tested, and every claim is supported by evidence available under NDA during due diligence.

100%	AES-256	Zero	<72h
Australian data residency for in-scope records	Envelope encryption at rest, HSM-backed keys	Standing production access; all elevation is just-in-time	Statutory breach notification pathway, rehearsed

Five commitments to a government buyer

- **Sovereignty is non-negotiable.** In-scope personal information is stored and processed in Australian regions. Offshore access is denied by default and permitted only where an agency has expressly approved it in the contract schedule.
- **Zero trust, not perimeter trust.** Every request — human or machine — is authenticated, authorised, and logged against an explicit policy. There is no trusted internal network.
- **Cryptography is engineered for the next decade.** TLS 1.3 in transit, AES-256-GCM at rest, field-level encryption for identity documents, and hybrid post-quantum key exchange on our edge to defend against harvest-now-decrypt-later collection.
- **AI is governed, not assumed.** Customer data is never used to train third-party foundation models. Model interactions are isolated, prompt-injection tested, PII-minimised before inference, and consequential outputs remain under registered-agent human review.
- **Assurance is independent.** Annual CREST/OSCP-led penetration testing, continuous vulnerability management, an ISO/IEC 27001 and SOC 2 aligned control set, and contractual audit rights for the agency.

Why this matters for immigration workloads

Immigration data is a standing target for state-aligned actors, organised document fraud, and identity-theft syndicates. A breach is not merely a privacy incident — it can expose visa applicants, their families, and in some cases people who have fled persecution. Our control design assumes a determined, well-resourced adversary rather than opportunistic crime.

SECTION 2

Scope, Systems & Data Handled

This dossier covers the VisaChief.com production platform and the services an agency would consume under contract. Corporate IT is in scope only where it can reach production data.

2.1 Systems in scope

System	Function	Sensitivity
Public web & eligibility engine	Anonymous visa eligibility assessment and route mapping	Low — no identity documents
Application wizard & document vault	Collection, storage and verification of applicant evidence including passports and identity documents	**Highest**
Agent & caseworker portal	Registered-agent review, lodgement preparation, case notes	High
Enterprise / agency integration layer	APIs, SSO, webhooks and bulk case exchange with institutional clients	High
AI assistance services	Document classification, completeness checking, drafting support, applicant guidance	High — mediated access
Analytics & reporting	Aggregated operational reporting on de-identified data	Low

2.2 Categories of personal information

Category	Examples	Treatment
Identity documents	Passport bio-pages, national ID, birth and marriage certificates	Field-level encryption; access on documented case need only
Biometric-adjacent	Compliant photographs, signature images	Segregated store; never sent to third-party models
Sensitive information (APP def.)	Health declarations, criminal history declarations, religious or political grounds in protection matters	Explicit consent; elevated access controls; extended audit
Financial evidence	Bank statements, payslips, sponsorship undertakings	Encrypted; masked in all non-production contexts
Contact & account	Name, address, email, phone, authentication material	Standard PII controls; credentials hashed with memory-hard KDF
Case metadata	Status, timestamps, agent actions, correspondence	Immutable audit trail; retained per disposal authority

Out of scope

VisaChief.com does not act as a decision-maker. Visa outcomes are determined solely by the relevant government authority. Where lodgement occurs, a registered migration agency in our partner network completes final review. This dossier therefore addresses custodianship and processing security, not adjudication.

SECTION 3

Governance, Risk & Compliance

Security is owned at executive level. The Chief Technology Officer is accountable for the information security management system; a Privacy Officer is separately accountable for obligations under the *Privacy Act 1988* (Cth). Risk is reviewed on a fixed cycle and on material change, with a documented risk register, treatment plans and named owners.

3.1 Obligations we design against

Instrument	Relevance	How we address it
Privacy Act 1988 (Cth) & Australian Privacy Principles	Collection, use, disclosure, security and access to personal information	APP-mapped privacy policy, collection notices, APP 11 security controls, APP 12 access process
Notifiable Data Breaches scheme	Mandatory assessment and notification of eligible breaches	30-day assessment clock with a 72-hour internal target; rehearsed OAIC notification pathway
Privacy and Other Legislation Amendment reforms	Statutory tort for serious invasion of privacy; automated-decision transparency	Automated-decision register; transparency statements; human review of consequential outputs
Migration Act 1958 & MARA Code of Conduct	Confidentiality and record-keeping duties of registered agents	Agent-scoped access, per-case authorisation, tamper-evident case records
PSPF and the Information Security Manual	Baseline expectations of Commonwealth entities and their providers	Control set mapped to ISM controls for OFFICIAL and OFFICIAL:Sensitive handling
Essential Eight (ACSC)	Mitigation baseline commonly required in government contracts	Assessed against Maturity Level targets; gap plan available under NDA
EU GDPR / UK GDPR	Applicants and agency staff located offshore	Lawful basis records, DPIA process, transfer mechanisms, data-subject rights workflow
ISO/IEC 27001, SOC 2 Type II	Recognised third-party assurance	Control set built to these frameworks; certification roadmap at 3.3
ISO/IEC 42001 & NIST AI RMF	Governance of AI systems	AI management system, model register, and evaluation regime — see Section 8

3.2 Control framework

Our control library is expressed once and mapped many ways, so that an agency assessor can receive evidence in the framework they already use rather than a translation exercise.

- **Primary library:** ISO/IEC 27001:2022 Annex A (93 controls), each with an owner, implementation statement, and evidence artefact.
- **Cross-maps maintained:** ISM controls (OFFICIAL / OFFICIAL:Sensitive), Essential Eight maturity, SOC 2 Trust Services Criteria, NIST CSF 2.0 functions, and CIS Critical Security Controls v8.
- **Statement of Applicability** is a living document; exclusions are justified in writing and reviewed at each cycle.
- **Policy suite** covers information security, acceptable use, access control, cryptography, secure development, change management, incident response, business continuity, supplier security, data retention, privacy, and AI use. Policies are versioned and acknowledged annually.

3.3 Assurance roadmap

We state assurance status plainly. Nothing below is claimed as achieved until an independent party has issued a report or certificate, and current artefacts are provided on request.

Assurance activity	Status	Evidence available
Independent penetration test (application + infrastructure)	Recurring — annual minimum, plus on major release	Executive summary and remediation register
Continuous vulnerability scanning & dependency monitoring	Operating	Scan cadence, SLA adherence, open-finding aging report
ISO/IEC 27001 certification	Roadmap — controls implemented, certification scheduled	Statement of Applicability, internal audit results
SOC 2 Type II	Roadmap — readiness assessment stage	Control matrix and readiness report
IRAP assessment	Available on agency requirement, scoped to the engagement	Scoping proposal on request
Essential Eight maturity assessment	Operating — self-assessed, independently validated on request	Maturity scorecard with gap plan
Privacy Impact Assessment	Completed for core platform; refreshed per material change	PIA report and treatment actions
Public vulnerability disclosure programme	Operating	Policy, intake channel, response metrics

Evidence pack

A due-diligence pack — Statement of Applicability, control matrix with framework cross-maps, current penetration-test summary, sub-processor register, architecture diagrams, incident response plan, business continuity test results and insurance certificates — is released under NDA within five business days of request.

SECTION 4

Data Sovereignty & Residency

Sovereignty is the first question a public-sector buyer asks, and the one most often answered vaguely. Our position is specific.

Question	VisaChief.com position
Where is in-scope personal information stored?	Australian cloud regions (Sydney and Melbourne availability zones) for primary and replica storage. Backups remain within Australian territory.
Where is it processed?	Compute, queues, search indexes and caches are pinned to Australian regions. Region pinning is enforced by policy-as-code, not by convention — deployments to non-approved regions fail at the control plane.
Can offshore staff access it?	Denied by default. Any offshore support access requires a named agency approval, is time-boxed, brokered through a session-recorded access path, and is reported in the access log provided to the agency.
Are sub-processors offshore?	The sub-processor register names every processor, its role, its location and its data categories. Agencies may veto sub-processors for their tenant under contract.
What about foreign-government access requests?	We maintain a law-enforcement request policy: requests are legally reviewed, narrowed where possible, resisted where improper, and the affected agency is notified unless legally prohibited. A transparency summary is available on request.
Is data commingled with other customers?	Logical isolation with tenant-scoped encryption keys and row-level authorisation. Dedicated infrastructure or a segregated tenancy is available for agency workloads.

4.1 Enforcement mechanisms

- Cloud organisation policy denies resource creation outside approved Australian regions across all accounts, including sandbox.
- Infrastructure-as-code is scanned pre-merge; a region violation is a hard build failure.
- Storage buckets and databases carry residency tags; a daily reconciliation job alerts on any untagged or out-of-region asset.
- Egress from production to the public internet is restricted to an allow-list of destinations, logged in full, and reviewed monthly.

SECTION 5

Identity & Access Management

We operate on the assumption that credentials will be phished and endpoints will be compromised. Access controls are therefore designed so that a stolen password, a stolen session, or a compromised laptop is insufficient to reach applicant data.

5.1 Workforce access

Control	Implementation
Phishing-resistant MFA	FIDO2 / WebAuthn hardware keys and passkeys are mandatory for all staff and contractors. SMS and push-approval factors are disabled for privileged paths.
Single sign-on	All internal systems are behind SSO with conditional access on device posture, location and risk signal. Legacy authentication protocols are blocked.
Zero standing privilege	No engineer holds persistent production access. Elevation is just-in-time, ticket-linked, peer-approved, time-boxed, and session-recorded.
Least privilege & separation of duties	Role-based access refined by attribute-based policy (case assignment, jurisdiction, data category). Deployment approval and code authorship cannot be the same person for production changes.
Device trust	Managed, disk-encrypted endpoints with EDR, screen-lock, patch enforcement and remote wipe. Unmanaged devices cannot obtain a production session.
Access review	Quarterly recertification by system owner; immediate revocation on role change; automated deprovisioning tied to the HR system within one hour of termination.
Break-glass	Two-person, sealed, alarmed on use, and reviewed by the CTO within 24 hours.

5.2 Applicant and agency-user access

- Passwords are hashed with a memory-hard function (Argon2id) and checked against breached-credential corpora at set and at login.
- Multi-factor authentication is available to all applicants and enforceable by policy for agency tenants; passkeys are supported.
- Enterprise tenants may federate via SAML 2.0 or OIDC with SCIM provisioning, so an agency's own joiner-mover-leaver process governs platform access directly.
- Sessions are short-lived, bound to device and network context, invalidated on privilege change, and terminated on anomaly. Concurrent-session limits and geo-velocity checks are enforced.
- Every access to an identity document is written to an append-only audit record naming the actor, case, purpose and timestamp. Agencies can subscribe to this feed for their own tenancy.

Machine identity

Service-to-service authentication uses short-lived, workload-attested credentials with mutual TLS. Long-lived API keys are not used inside the platform. External integration credentials are scoped, rotatable by the agency at will, and revocable within seconds.

SECTION 6

Cryptography & Key Management

Encryption is applied in depth rather than at a single layer, and the key hierarchy is designed so that compromise of storage, of a backup, or of a single service does not yield plaintext.

Layer	Control
In transit (external)	TLS 1.3 only, with modern cipher suites, HSTS preloading, OCSP stapling, and certificate transparency monitoring. TLS 1.0/1.1 and all deprecated suites are refused.
In transit (internal)	Mutual TLS between every service, with automatically rotated workload certificates and a service mesh enforcing identity-based authorisation.
At rest (storage)	AES-256-GCM full-volume and object encryption across databases, object stores, queues, search indexes and backups.
At rest (field level)	Identity documents, biometric-adjacent images and sensitive declarations receive an additional application-layer encryption envelope with per-tenant data keys, so a database compromise alone does not expose passport data.
Key custody	Keys are generated and held in FIPS 140-2/140-3 validated hardware security modules. Key material is never exported in plaintext, and no individual can extract a key.
Key rotation	Automatic annual rotation of data-encryption keys, quarterly for signing keys, and immediate rotation on suspicion of compromise. Re-encryption is performed online.
Customer-managed keys	Available for agency tenants, including hold-your-own-key arrangements that allow the agency to revoke access to its own data unilaterally.
Secrets	Centralised secret manager with dynamic, short-lived database credentials. Pre-commit and CI scanning blocks any secret from entering the repository.
Hashing & signing	SHA-256/SHA-384 for integrity; Ed25519 for artefact signing; Argon2id for credential storage. MD5 and SHA-1 are prohibited platform-wide.

6.1 Post-quantum readiness

Immigration records retain their sensitivity for decades — a passport scan harvested today is still damaging in 2040. That makes *harvest-now, decrypt-later* collection a live threat rather than a theoretical one, and it is why our cryptographic roadmap is already moving.

- **Hybrid key exchange at the edge.** Our TLS termination supports hybrid post-quantum key agreement (X25519 combined with ML-KEM, per NIST FIPS 203), so session keys resist both classical and future quantum attack while remaining interoperable with today's clients.
- **Cryptographic inventory.** We maintain a machine-readable register of every algorithm, key length and protocol in use — the precondition for any credible migration.
- **Crypto-agility by design.** Algorithms are referenced through an abstraction layer, so a primitive can be replaced without re-architecting the application.
- **Signature migration path.** ML-DSA (FIPS 204) is on the roadmap for artefact and document signing, tracked against ACSC and NIST guidance, with long-lived signatures prioritised first.

SECTION 7

Application & Product Security

Security is enforced in the pipeline, not requested of developers. A change cannot reach production without passing the gates below.

7.1 Secure development lifecycle

Stage	Gate
Design	Threat modelling for new features touching personal information or authentication; privacy impact triage; abuse-case review.
Code	Mandatory peer review; no direct commits to protected branches; signed commits; secure coding standards aligned to OWASP ASVS.
Build	SAST, software composition analysis, secret scanning, container image scanning, and infrastructure-as-code policy checks. Critical findings block the build.
Provenance	Reproducible builds with a generated SBOM (CycloneDX) and signed provenance attestations aligned to SLSA. Only signed artefacts are admitted to production.
Test	Automated security regression suite covering authentication, authorisation, tenancy isolation and file handling; DAST against a production-like environment.
Release	Change approval with separation of duties; progressive rollout; automated rollback on error-budget breach.
Run	Runtime protection, continuous configuration drift detection, and immutable infrastructure — servers are replaced, not patched in place.

7.2 Application defences

- OWASP Top 10 and API Top 10 controls verified by test, including parameterised data access, output encoding, strict content security policy, and anti-CSRF protections.
- Object-level authorisation is enforced centrally — the most common cause of data exposure in multi-tenant systems is checked in one place and tested continuously.
- Uploaded documents are treated as hostile: type verification, size limits, multi-engine malware scanning, content disarm and reconstruction for office formats, quarantine on suspicion, and rendering from an isolated origin with no ambient credentials.
- Rate limiting, bot management and adaptive challenge protect enumeration-prone endpoints such as eligibility checks and status lookup.
- Web application firewall and managed DDoS protection sit in front of all public endpoints.
- Non-production environments never contain live personal information; test data is synthetic or irreversibly de-identified.

7.3 Vulnerability management

Severity	Remediation target (production)	Interim measure
Critical	24 hours	Immediate mitigation, virtual patch or feature disablement
High	7 days	Compensating control and monitoring rule
Medium	30 days	Tracked with owner and due date
Low	90 days or next planned release	Backlog with periodic review

SECTION 8

AI Assurance & Model Security

VisaChief.com is an AI-native platform, and AI introduces failure modes that traditional security reviews do not cover. We treat models as an untrusted, non-deterministic component operating inside a governed boundary.

8.1 Data protection in AI processing

- **No training on customer data.** Contracts with model providers prohibit the use of our inputs or outputs to train, fine-tune or improve their models. Zero-data-retention processing is used where the provider offers it.
- **Minimisation before inference.** Personal information is reduced to what the task requires; direct identifiers are redacted or tokenised before a prompt leaves our boundary, and re-hydrated only within our own trust zone.
- **Biometric-adjacent exclusion.** Passport photographs and signature images are not sent to third-party general-purpose models.
- **Residency for inference.** Where an agency requires it, inference is served from Australian-region endpoints or from models hosted within our own tenancy.

8.2 Model and pipeline security

Risk	Control
Prompt injection (direct and indirect)	Untrusted content — uploaded documents, third-party web content, applicant free text — is structurally separated from instructions, never granted tool authority, and processed by models with no standing access to data outside the case. Injection test suites run in CI.
Excessive agency	Model outputs cannot invoke privileged actions. Any state change is executed by deterministic application code with its own authorisation check, and consequential steps require human confirmation.
Sensitive information disclosure	Output filtering and tenancy assertion on every response; retrieval is scoped to the requesting case by policy, not by prompt instruction.
Hallucination in a regulated domain	Retrieval grounded in versioned, citable source material; confidence thresholds; explicit refusal behaviour; and mandatory registered-agent review before lodgement. The platform gives preliminary information, not immigration advice.
Model supply chain	Model and version pinning, provider assurance review, change notification, and regression evaluation before any version is promoted.
Denial of wallet / abuse	Per-tenant quotas, cost anomaly alerting and circuit breakers.
Bias and fairness	Evaluation across nationality, language and cohort segments; documented outcomes; corrective action tracked as a defect.

8.3 AI governance

- An AI management system aligned to ISO/IEC 42001 and the NIST AI Risk Management Framework, consistent with Australia's AI Ethics Principles and the Voluntary AI Safety Standard.
- A model register recording every deployed model, its purpose, data flows, evaluation results, human-oversight design and accountable owner.
- Automated-decision transparency: applicants are told where AI assists their matter, and no adverse consequential decision is made by a model without human review.
- Full prompt-and-response logging within our boundary for investigation, with the same retention, encryption and access controls as case data.

SECTION 9

Infrastructure & Network Security

Domain	Control
Architecture	Segmented into public edge, application, data and management planes. The data plane has no route to the internet; all outbound traffic is proxied and allow-listed.
Private connectivity	Databases and internal services are reachable only through private endpoints. No production data store carries a public address.
Micro-segmentation	Default-deny network policy between workloads; each service may talk only to declared dependencies.
Hardening	CIS-benchmarked base images, minimal distroless containers, read-only file systems, non-root execution, and no interactive shell in production images.
Patching	Automated base-image rebuilds on upstream advisory; immutable redeployment rather than in-place patching; emergency patch path for critical advisories.
Runtime defence	Behavioural runtime detection on hosts and containers, file-integrity monitoring, and automatic isolation of anomalous workloads.
Administration	No SSH into production. Administration occurs through an audited control plane; where a session is unavoidable it is brokered, recorded and reviewed.
Edge protection	Global anycast edge with DDoS absorption, TLS termination, WAF, bot management and geo-policy controls.
Configuration assurance	Continuous cloud security posture management with automatic remediation of drift; misconfiguration is treated as a security incident.

Tenancy isolation

Isolation is enforced at four layers simultaneously: network policy, service-level authorisation, row-level database policy, and per-tenant encryption keys. Cross-tenant access attempts are automated test cases in the release pipeline, not assumptions.

SECTION 10

Detection, Response & Breach Notification

10.1 Monitoring

- Centralised logging from application, infrastructure, identity, and cloud control planes into a SIEM with correlation and behavioural analytics.
- Security logs are written to append-only, immutable storage with independent retention, so an attacker with production access cannot erase their trail.
- Detection content covers credential abuse, impossible travel, privilege escalation, mass document access, data-exfiltration patterns, and anomalous AI usage.
- Alerting is triaged 24×7 with defined escalation to on-call security engineering.

10.2 Incident response

Phase	Commitment
Detect & triage	Severity assigned within 30 minutes of alert for critical categories.
Contain	Isolation of affected identity, workload or tenant path as the first action; credential and key rotation initiated immediately.
Notify (agency)	Initial notification to the affected agency within 24 hours of confirming an incident involving its data, with updates at agreed intervals.
Notify (regulator)	Assessment under the Notifiable Data Breaches scheme commenced immediately; OAIC and affected individuals notified as soon as practicable, with a 72-hour internal readiness target and full compliance with the 30-day statutory assessment period.
Eradicate & recover	Root-cause removal, integrity verification and staged restoration with heightened monitoring.
Review	Blameless post-incident review with corrective actions tracked to closure; report shared with the affected agency.

- The incident response plan is exercised at least annually, including a tabletop with executive participation and a technical simulation of a data-exfiltration scenario.
- Retained external digital forensics and incident response capability is available on call.
- Cyber liability insurance is maintained; certificates of currency are provided on request.
- A dedicated agency incident contact and escalation matrix is agreed at contract signature.

SECTION 11

Resilience, Backup & Continuity

Capability	Design	Target
Availability	Multi-availability-zone deployment with automated failover and no single point of failure in the request path	99.9% monthly for the production platform
Recovery point objective	Continuous transaction-log shipping with point-in-time recovery	<= 15 minutes
Recovery time objective	Automated infrastructure rebuild from code plus restore	<= 4 hours for core case-management services
Backup regime	Encrypted, versioned backups with immutability locks; a copy held in a separate account with distinct credentials	Daily full, continuous incremental
Ransomware resistance	Write-once backup retention that cannot be shortened or deleted by production credentials	Independent deletion control
Restoration testing	Scheduled restore rehearsals into an isolated environment with integrity verification	At least quarterly
Business continuity	Documented plan covering personnel loss, provider outage, third-party failure and premises unavailability	Reviewed and exercised annually
Exit & portability	Full export of an agency's data in open, documented formats, plus certified destruction of residual copies	Within 30 days of request

No lock-in by obscurity

An agency's data belongs to the agency. Export is a supported, tested product capability with documented schemas — not a bespoke professional-services engagement — and destruction is evidenced by a signed certificate covering backups and replicas.

SECTION 12

Supply Chain & Third-Party Risk

Most modern breaches arrive through a supplier. Our third-party controls are therefore treated with the same rigour as our own.

- **Register and transparency.** A current sub-processor register lists each provider, its purpose, the data categories it touches, and its hosting location. Agencies are notified before a new sub-processor handling personal information is engaged, with a right to object.
- **Risk-tiered due diligence.** Providers touching personal information undergo security review before engagement: certification evidence, penetration-test attestation, breach history, sub-processing chain and residency.
- **Contractual flow-down.** Confidentiality, security standards, breach notification timelines, audit rights, residency obligations and deletion duties are imposed contractually on every provider in scope.
- **Registered agent network.** Partner migration agencies are bound by confidentiality undertakings, access is scoped to assigned cases only, and every document view is logged and attributable.
- **Continuous monitoring.** Provider security posture, advisories and incident disclosures are monitored; material degradation triggers reassessment.
- **Software supply chain.** Dependencies are pinned, provenance-verified and continuously scanned; an SBOM is maintained per release and can be supplied to the agency.
- **Concentration risk.** Critical dependencies have documented alternates and, where practical, tested migration paths.

SECTION 13

Personnel & Physical Security

Control	Implementation
Pre-employment screening	Identity verification, right-to-work, reference and qualification checks, and a National Police Check for all personnel with access to personal information.
Government clearance	Personnel can be nominated for Australian Government security clearance where an engagement requires it.
Binding obligations	Confidentiality and acceptable-use agreements executed before access; obligations survive termination.
Training	Security and privacy induction, annual refresher, role-specific secure development training, and continuous phishing simulation with remediation.
Insider threat	Least privilege, separation of duties, behavioural monitoring on sensitive data stores, and mandatory anomaly review — designed so that unusual access is visible even when it is authorised.
Offboarding	Access revoked within one hour of termination; asset return; exit attestation.
Physical	Production infrastructure resides in certified data centres operated by major cloud providers with biometric access control, 24×7 guarding and full CCTV. VisaChief personnel have no physical access to production hardware. Corporate premises use access control, clear-desk policy and secure destruction of physical media.

SECTION 14

Privacy by Design & Data Lifecycle

14.1 Principles in practice

- **Collect less.** Each field is justified against a lawful purpose; optional data is clearly marked; we do not collect sensitive information unless the visa route requires it.
- **Tell people plainly.** Layered collection notices explain what is collected, why, who receives it and how long it is kept — in plain language, at the point of collection.
- **Separate by purpose.** Analytics operate on de-identified or aggregated data; marketing systems never receive identity documents or sensitive declarations.
- **Give control.** Access, correction, export and deletion requests are handled through a documented workflow with identity verification and statutory timeframes.
- **Assess before building.** Privacy impact assessment is triggered by any new processing of personal information, new sub-processor, or new automated decision.

14.2 Retention and destruction

Data	Retention approach
Active case records and evidence	Retained for the life of the matter plus the period required by professional and record-keeping obligations, then destroyed.
Identity documents	Retained only while required for the matter; deletion on completion where no legal obligation compels retention.
Agency-tenant data	Retention configurable by the agency, including shorter periods and records-authority-aligned schedules; deletion or transfer to the agency at contract end.
Security and audit logs	Retained for a defined period on immutable storage to support investigation, then automatically expired.
Anonymous eligibility checks	No identity documents collected; retained in aggregate form only.
Backups	Deleted records are purged from backups on the documented backup cycle; the residual window is disclosed and contractually bounded.

Destruction is irreversible: cryptographic erasure of tenant keys is used alongside logical deletion, so residual ciphertext is unrecoverable. Certificates of destruction are issued on request.

SECTION 15

Independent Assurance & Testing

- **Penetration testing.** Independent testing of the application, API and cloud infrastructure at least annually and before any major architectural change, conducted by appropriately accredited testers. Findings are tracked to closure against the SLAs in Section 7.3; an executive summary and remediation status are shared with agency clients.
- **Red teaming.** Objective-based exercises against realistic adversary tradecraft, including social engineering with executive authorisation, to test detection and response rather than configuration.
- **Continuous scanning.** Authenticated and unauthenticated scanning of external and internal surfaces, dependency monitoring, container and IaC scanning integrated into the pipeline.
- **Vulnerability disclosure.** A published policy with a safe-harbour statement, a monitored intake channel, acknowledgement within two business days, and coordinated disclosure.
- **Internal audit.** Scheduled control testing against the Statement of Applicability with findings reported to the executive.
- **Agency audit rights.** Contracts provide for the agency to audit — or to appoint an auditor for — controls relevant to its data, on reasonable notice and subject to confidentiality.

SECTION 16

Shared Responsibility Model

Clear demarcation prevents the gaps where incidents happen.

Responsibility	VisaChief.com	Agency / Client
Platform, application and infrastructure security	Owns	Assures
Data residency enforcement	Owns	Specifies requirement
Encryption and key management	Owns (customer-managed keys optional)	Owns key policy where CMK/HYOK is elected
Identity federation and user lifecycle	Provides SSO/SCIM capability	Owns its directory, MFA policy and joiner-mover-leaver process
Role assignment and least privilege within the tenant	Provides the model	Owns the assignment
Accuracy and lawfulness of data supplied	Processes as instructed	Owns collection notice and lawful basis
Retention schedule for the tenant	Enforces configured policy	Sets the schedule
Incident detection on the platform	Owns	Receives notification and log feed
Incident response within the agency environment	Supports	Owns
Endpoint security of agency users	Enforces device conditions where federated	Owns

SECTION 17

Service Commitments

Commitment	Target
Production availability	99.9% monthly, measured on the core case-management service
Planned maintenance	Notified at least 5 business days in advance; performed in agreed low-impact windows
Critical security patch deployment	Within 24 hours of a validated fix
Security incident notification to the agency	Within 24 hours of confirmation
Security questionnaire response	Within 10 business days
Evidence pack release (under NDA)	Within 5 business days
Data export request	Within 30 days, in open documented formats
Certificate of destruction	Within 30 days of confirmed deletion

SECTION 18

Contact & Vulnerability Disclosure

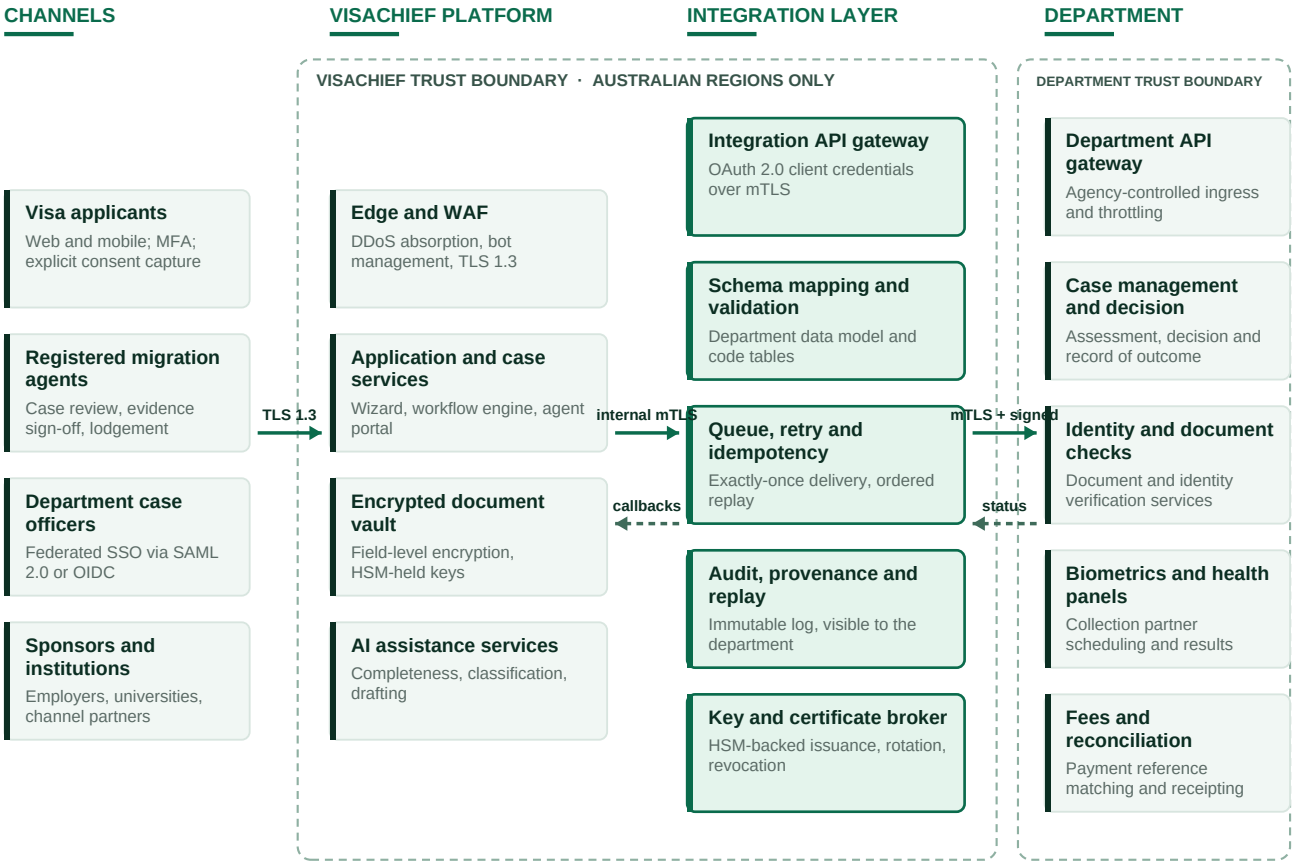
Purpose	Channel
Security enquiries, questionnaires and evidence requests	security@visachief.com
Privacy enquiries, access and correction requests	privacy@visachief.com
Vulnerability reports (safe harbour applies)	security@visachief.com — encrypted submission supported
Incident escalation (contracted agencies)	Escalation matrix issued at contract signature
Procurement and commercial	partnerships@visachief.com
Web	https://visachief.com

ANNEX A

Government Integration Architecture

This annex describes how VisaChief.com connects to a department's visa processing environment. The connection is mediated by a dedicated component — the **VisaChief Government Integration Layer** — which exists so that the department integrates with one hardened, contract-bound interface rather than with the platform's internal services.

The architecture below is a reference pattern. The specific systems, protocols and interconnect method are agreed with the department during design authority review and recorded in the integration schedule to the contract.



- Every cross-boundary call is mutually authenticated with certificate pinning; payloads are signed, versioned and idempotent.
- The department controls its own ingress. VisaChief holds no credential that can write directly to a departmental data store.
- Personal information never leaves Australian regions; the integration layer is the only component permitted to egress to the department.

Figure A.1 — Reference architecture: VisaChief Government Integration Layer

A.1 Lodgement data flow

The sequence below is the standard path for a prepared application. Each step is logged with an immutable, department-visible audit record.

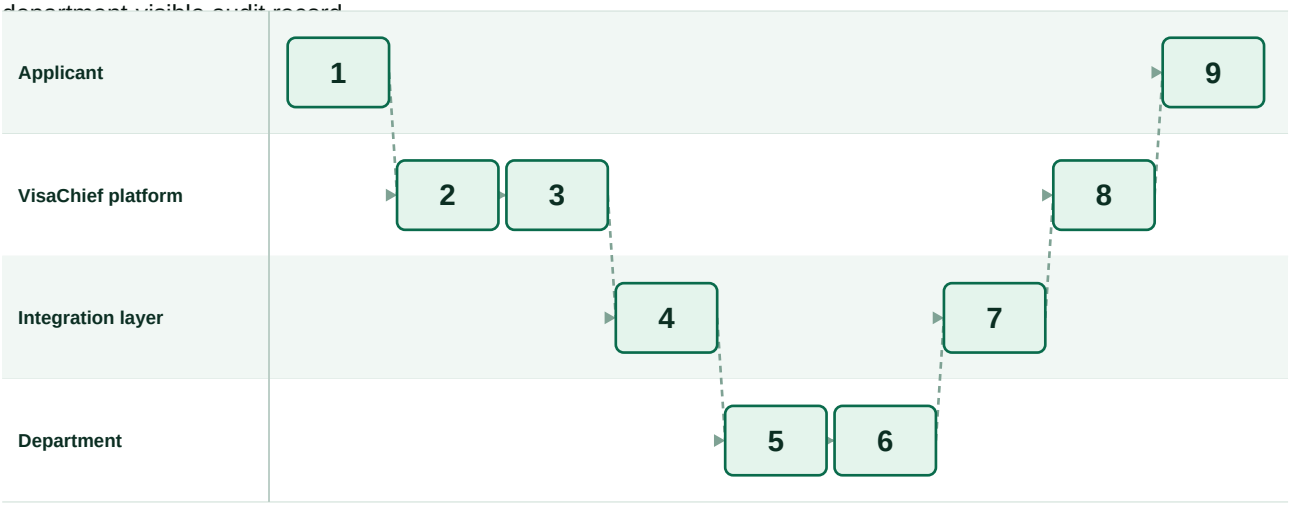


Figure A.2 — Lodgement sequence across trust boundaries

Step	Action	Control applied
1	Applicant submits evidence and grants explicit consent	Consent recorded; upload scanned, type-verified and quarantined
2	Vault stores documents; AI completeness check runs	Field-level encryption; identifiers minimised before inference
3	Registered migration agent reviews and signs off	Human decision point; agent identity bound to the case record
4	Integration layer builds and signs the lodgement package	Schema validation against the department model; payload signed
5	Package transmitted to the department gateway	Mutual TLS, certificate pinning, idempotency key, retry with backoff
6	Department acknowledges receipt and assigns a reference	Acknowledgement persisted to the immutable audit log
7	Status and requests for information returned	Signed callback or authenticated poll — department's election
8	Platform updates the case and notifies the agent	Tenancy-scoped authorisation on every read
9	Applicant notified of status; decision recorded	Decision attributed to the department, never to VisaChief

A.2 Integration patterns supported

Pattern	Protocol	Typical use	Assurance
Synchronous API	REST/JSON over HTTPS with OAuth 2.0 client credentials and mTLS	Eligibility checks, status lookup, reference data	Per-call authentication, rate limits, full request logging
Asynchronous submission	Queued POST with idempotency key and signed payload	Lodgement packages and document bundles	Exactly-once delivery, ordered replay, acknowledgement receipts
Event callback	Signed webhook to a VisaChief endpoint, or authenticated poll	Status changes, requests for further information	Signature verification, replay window, poll fallback if the department disallows inbound
Bulk exchange	SFTP with PGP-encrypted payloads, or object-store handoff	Batch reconciliation and periodic reporting	Key-pair authentication, manifest checksums, transfer receipts
Identity federation	SAML 2.0 or OIDC with SCIM provisioning	Department staff access to the case portal	Department's own directory and MFA policy govern access
Reference data sync	Versioned pull of code tables and legislative instruments	Visa subclasses, fees, document checklists	Version pinning and change notification so outputs remain reproducible

A.3 Interconnect options

The department elects the connectivity model. All three carry the same application-layer controls; they differ in network exposure.

Option	Description	When it suits
Private interconnect	Dedicated cloud interconnect or private peering between the department's network and the VisaChief integration layer, with no traffic traversing the public internet	Highest-assurance workloads and departments with an existing cloud interconnect
Mutual TLS over the public internet	IP allow-listing, certificate pinning and signed payloads across a public path	Fastest to establish; suits pilots and lower-volume integrations
Gateway-brokered	Both parties integrate through a departmental or whole-of-government API gateway	Where the department mandates a central integration platform

A.4 Responsibilities at the boundary

Item	VisaChief.com	Department
Integration layer build and operation	Owns	Reviews and approves design
Interface specification and data model	Implements to specification	Owns the specification and code tables
Certificates and key rotation	Issues and rotates its own; supports pinning	Issues and rotates its own
Ingress control and throttling	Respects published limits	Owns
Payload content accuracy	Validates against schema and completeness rules	Owns assessment and decision
Audit log of exchanges	Produces immutable log and provides access	Retains per its own records authority

Item	VisaChief.com	Department
Incident notification across the boundary	Notifies within 24 hours of confirmation	Notifies per its own policy
Environment provisioning	Provides sandbox, staging and production	Provides test endpoints and test data

Onboarding path

Design authority review and interface agreement, then sandbox connectivity and certificate exchange, then conformance testing against department test cases, then a security assessment and penetration test of the integration, then a limited production pilot with agreed volume caps before full cutover. Each gate has documented exit criteria signed by both parties.

Statement of intent. VisaChief.com does not treat security as a compliance exercise to be survived at procurement. The controls described here exist because the people who use this platform are handing us the documents that define their identity and, in many cases, their future. We hold that data as a custodian, we expect to be audited on it, and we publish this dossier so that an agency can hold us to a specific standard rather than a general assurance.

This document describes VisaChief.com's security programme as at the issue date and is provided for evaluation purposes. It is commercial-in-confidence and does not itself form a contractual warranty; binding obligations are those set out in the executed agreement, its security schedule and its data processing terms. Certification statuses are as recorded in Section 3.3 and current evidence is available on request. VisaChief.com provides preliminary information and application preparation services; visa decisions are made solely by the relevant government authority.