



ALASTRONIX, LLC

Invilex Compliance & Security Report

Overview of security controls, compliance frameworks, and data protection practices.

October 19, 2026

PUBLIC

Invilex is pre-launch. "Implemented" means built into our code and infrastructure; it will be running for customers at launch. "Planned" items are designed but not yet built.

<https://trust.invilex.ai>
security@invilex.ai

Compliance Frameworks

Framework	Status	Description
SOC 2	PLANNED	Alastronix, LLC is building the Invilex platform against the AICPA Trust Services Criteria for Security, Availability, Confidentiality, and Processing Integrity. A SOC 2 audit has not started.

Data Protection

6/6 controls implemented

Control	Status	Description
Dedicated Tenancy per Firm	IMPLEMENTED	Each firm runs in its own Oracle Cloud Infrastructure tenancy with its own network, key vault, database, storage, and identity domains. No data store is shared between firms.
Encryption at Rest	IMPLEMENTED	Cached case data and sensitive fields (names, case numbers, staff notes, appointment details) are encrypted in the application with AES-256-GCM. Their keys are wrapped by an HSM-protected AES-256 master key in OCI Vault that never leaves the HSM. Journal entries and chat transcripts are stored in OCI Object Storage, encrypted at rest by Oracle with Oracle-managed keys.
Encryption in Transit	IMPLEMENTED	All traffic reaches Invilex over TLS through Cloudflare. Cloudflare connects to the load balancer over TLS 1.2 with forward-secret AES-GCM cipher suites. The load balancer and application communicate inside a private subnet. Calls to Oracle services and third parties use HTTPS.
Short-Lived Case Cache	IMPLEMENTED	The firm's case management system stays the system of record. Case data Invilex caches is encrypted under keys that are destroyed every night, and a firm can revoke a case's cached data on demand. Every key destruction is audited.
Tamper-Evident Pain Journal	IMPLEMENTED	Journal entries are signed on the client's phone with a non-exportable hardware key, linked in hash chains, and anchored hourly by a signature from an HSM key in OCI Vault. They are stored in write-once buckets locked for five years.
Retention by Data Class	IMPLEMENTED	Case caches are kept about one day. Staff notes are destroyed 12 months after a case closes. Chat transcripts are kept six years after closure by default (configurable by the firm). Journal entries are locked for five years. Audit evidence is locked for two years.

AI & Privacy

2/5 controls implemented

Control	Status	Description
AI Inside the Firm Tenancy	PLANNED	The assistant's model will run on OCI Generative AI in the firm's own tenancy and region. Invilex does not train models on customer data. Zero-data-retention terms are being confirmed with Oracle.
Answers Limited to the Client's Case	PLANNED	The assistant answers only from the client's own published case information and firm-approved knowledge entries. It never sees staff-only records, and questions that call for legal advice go to the firm's staff.
Legal-Advice Safety Check	PARTIAL	A fixed phrase check reviews assistant answers and flags possible legal advice to the responsible attorney. An independent second-model review is planned.
Masking Before Escalation to Invilex	IMPLEMENTED	When an attorney sends an assistant answer to Invilex for review, a masking service on the same host removes the client, case parties, staff, case numbers, contact details, dates, addresses, medical terms, and long numbers before Invilex can read it.
On-Device Voice	IMPLEMENTED	Speech recognition and text-to-speech run on the client's phone. Audio never leaves the device.

Access Control

2/5 controls implemented

Control	Status	Description
Granular Staff Permissions	IMPLEMENTED	Sixteen permissions, each scoped to assigned cases, specific locations, or all cases. Grants and revocations are audited. Cases a person cannot access return "not found", so their existence is not revealed.
Staff Sign-In and MFA	PLANNED	Staff will sign in through a dedicated OCI Identity domain in the firm's tenancy, with multi-factor authentication required (authenticator app or email code; FIDO2 security keys for attorneys).
Client Sign-In	PARTIAL	Password plus a required second factor (authenticator app or email code; SMS is never a factor). Lockout after repeated failures, rate-limited sign-in, 30-minute access tokens, and one approved phone per client. Integration with the production identity domain is in progress.
No Standing Invilex Access	PARTIAL	Invilex's access into a firm tenancy is limited by policy to reading operational logs and masked incident reports. Hardware-key-only administrator sign-in, network restrictions, and an audited break-glass procedure are planned.
Least-Privilege Workloads	IMPLEMENTED	The application authenticates to Oracle services with resource principals, so there are no long-lived API keys. It cannot drop database tables, delete locked buckets, or delete secrets.

Infrastructure Security

4/5 controls implemented

Control	Status	Description
Network Isolation	IMPLEMENTED	Application instances run in a private subnet with no public IP addresses. The load balancer accepts HTTPS only from Cloudflare, and the application accepts traffic only from the load balancer.
Edge Protection	PARTIAL	Every firm domain is served through Cloudflare for TLS and DDoS protection. Web application firewall rules are being finalized.
Container Hardening	IMPLEMENTED	Containers run as non-root users from pinned base images and are deployed by image digest. Images are pulled with workload identity, so no registry credentials exist.
Infrastructure as Code	IMPLEMENTED	Each firm tenancy is defined in Terraform with automated tests. Vaults, keys, identity domains, and locked buckets are protected from accidental destruction.
Secret Management	IMPLEMENTED	Third-party credentials (case management, calendar, messaging) are stored in OCI Vault and never in images, configuration, or logs.

Application Security

2/5 controls implemented

Control	Status	Description
Automated Testing	IMPLEMENTED	Unit and integration tests cover encryption, key destruction, permissions, record visibility, transcript retention, and the client API. Infrastructure modules have their own test suites.
CI/CD and Code Scanning	PLANNED	A deployment pipeline with required peer review and passing tests, dependency and container scanning, signed images, and an SBOM for each release.
Upload and Webhook Validation	PARTIAL	Uploads are limited to JPEG, PNG, HEIC, and PDF up to 25 MB, with the type checked from file contents. Case management webhooks must carry a valid HMAC-SHA256 signature. Malware scanning of uploads is planned.
Threat Model	IMPLEMENTED	Documented threat model covering cross-firm exposure, unpublished content, journal tampering, log leakage, stolen phones, compromised staff accounts, CMS token theft, and prompt injection.
Penetration Testing	PLANNED	Annual third-party penetration test with tracked remediation.

Logging & Incident Response

2/4 controls implemented

Control	Status	Description
Audit Trail	IMPLEMENTED	About 70 kinds of security events (sign-ins, permission changes, publishing, transcript views, key destruction, device approvals, consent) are recorded without case content. Each event is written to the database and to a write-once, hash-chained stream anchored hourly.
Infrastructure Audit and Alerting	IMPLEMENTED	Oracle's tenancy audit log is archived to a bucket locked for two years. On-call is paged for destructive actions (deleting buckets, keys, policies, logs, or identity domains) and for unhealthy application instances.
Application Log Monitoring	PLANNED	Shipping application logs to OCI Logging and alerting on application events (failed key destruction, failed anchoring, delivery failures).
Incident Response Plan	PLANNED	A written incident response plan with an on-call rotation, customer notification procedure, and annual tabletop exercise.

Business Continuity

1/3 controls implemented

Control	Status	Description
High Availability	IMPLEMENTED	Two application instances run across availability domains with health checks and automatic restart. Either can carry the full load.
Second Region	PARTIAL	Each firm tenancy has a second OCI region with a locked bucket for transcript copies and a second master key. Replicating journal, evidence, database, and identity data to it is in progress.
Backups and Recovery Testing	PLANNED	Database backups to a locked bucket in the second region, with annual restore tests and failover drills.

Governance

0/4 controls implemented

Control	Status	Description
Security Policies	PLANNED	A written policy suite (information security, access, change management, vendor management, incident response) with annual review and risk assessment.
Personnel Security	PLANNED	Background checks and security training at hire and annually, with policy acknowledgments, for Invilex personnel.
Vendor Management	PLANNED	A subprocessor inventory, security terms in vendor contracts, and annual review of vendor security reports.
Data Processing Agreement	PLANNED	A customer data processing agreement for firms.

Subprocessors

Vendor	Purpose	Location
Oracle Cloud Infrastructure	Hosting for each firm's dedicated tenancy: compute, database, object storage, key vault, identity, and logging. Planned: AI models through OCI Generative AI.	United States
Cloudflare	DNS, TLS, and DDoS protection in front of every firm domain	Global (edge network)
Twilio	Planned: crisis alert texts and calls to firm contacts (a case reference only, no client details)	To be confirmed
Mailgun	Planned: invitation and staff notification email (no case content)	To be confirmed
Apple and Google	Planned: push notifications (generic text only) and app store distribution	To be confirmed
Clio	Firm-directed integration: syncs with the firm's own Clio account, its system of record	To be confirmed
Microsoft and Google calendars	Firm-directed integration: reads busy times from calendars staff choose to link (start and end times only)	To be confirmed

Published Documents

Document	URL
Privacy Policy	https://invilex.ai/privacy
Terms of Service	https://invilex.ai/terms