EVIDENCE BOUND

Security Addendum

Effective Date: January 2026 | Version 1.0

1. Introduction

This Security Addendum describes the security measures and practices that Evidence Bound implements to protect Customer Data processed in connection with the Evidence Bound service. This Addendum is incorporated into and forms part of the Master Services Agreement or Terms of Service between Provider and Customer.

2. Definitions

Customer Data means all data, including documents, files, and queries, that Customer uploads to or processes through the Service.

Personal Data means any information relating to an identified or identifiable natural person contained within Customer Data.

Security Incident means any unauthorized access, acquisition, use, or disclosure of Customer Data.

3. Security Program

3.1 Information Security Management

Provider maintains a comprehensive information security program designed to protect the confidentiality, integrity, and availability of Customer Data. This program includes:

- Dedicated security personnel responsible for security operations
- Written security policies and procedures reviewed annually
- Security awareness training for all personnel
- Regular risk assessments and security audits
- Incident response procedures and business continuity planning

3.2 Third-Party Audits and Certifications

Provider maintains or is pursuing the following third-party audits and certifications:

Certification	Status	Auditor
SOC 2 Type II	In Progress (Target Q3 2026)	TBD
ISO 27001	Roadmap (Target Q4 2026)	TBD
Penetration Testing	Annual	Independent Third Party

4. Technical Security Controls

4.1 Encryption

Provider implements the following encryption standards:

- Data in Transit: TLS 1.2 or higher for all network communications
- Data at Rest: AES-256 encryption for all stored Customer Data
- Key Management: Keys stored in dedicated key management systems
- HSTS: HTTP Strict Transport Security enabled on all web endpoints

4.2 Access Control

- Role-Based Access Control (RBAC) with principle of least privilege
- Multi-factor authentication (MFA) for all administrative access
- SSO integration via OIDC/SAML for Enterprise customers
- Quarterly access reviews and prompt deprovisioning
- Unique user IDs with prohibition on shared accounts

4.3 Network and Application Security

- Firewalls and network segmentation
- Intrusion detection and prevention systems
- DDoS protection and VPC isolation
- Static and dynamic application security testing
- Dependency and container image scanning in CI/CD

5. Data Handling

5.1 Data Isolation

All Customer Data is logically isolated using tenant identifiers (tenant_id) and matter identifiers (matter_id). Database queries are enforced to filter by these identifiers, preventing any cross-tenant or cross-matter data access.

5.2 Data Retention and Deletion

Customer Data is retained only as necessary to provide the Service. Customers may configure retention policies per tenant or matter. Upon termination, Provider will delete all Customer Data within thirty (30) days. Certificate of Destruction available upon request.

5.3 No Training on Customer Data

Provider does not use Customer Data to train, improve, or develop any machine learning or artificial intelligence models. Customer Data is used exclusively for providing the Service.

5.4 LLM Provider Data Handling

Provider maintains zero-retention agreements with underlying LLM providers. Prompts and responses are not retained beyond the API request. For On-Premise deployments, all LLM processing occurs locally with no external data transmission.

6. Audit and Logging

Provider maintains comprehensive audit logs including: user identification, timestamp, query text (excerpts redacted), documents accessed, LLM provider/model used, and response summary. Audit logs are append-only and exportable per matter or date range.

7. Security Incident Response

In the event of a Security Incident affecting Customer Data, Provider will: notify Customer within seventy-two (72) hours; provide information about the nature and scope; take steps to mitigate harm; cooperate with investigation requests; and provide a post-incident report.

8. Subprocessors

Category	Purpose	Data Processed
Cloud Infrastructure	Hosting and compute	All Customer Data
LLM Provider	AI text generation	Query prompts (zero-retention)
Observability	Monitoring and logging	Operational metrics (no PII)

Current subprocessor list maintained at bound.legal/security.

9. Customer Responsibilities

- Maintaining confidentiality of user credentials
- Configuring appropriate access controls within the Service
- Ensuring uploaded data complies with applicable laws
- Reviewing and verifying AI-generated outputs before reliance
- Reporting suspected security incidents promptly

10. Audit Rights

Upon reasonable written request (no more than once per year), Provider will make available SOC 2 Type II audit reports, penetration test summaries, and other compliance documentation.

Contact Information

Security inquiries: security@bound.legal

General inquiries: pilots@bound.legal

Website: bound.legal/security