MandateMind

Security & Data Handling Overview

Protecting Your Data with Transparency,
Encryption & Zero-Noise Architecture

Secure by Design	AWS-Hosted	AES-256 Encryption	SOC 2 Aligned

CONFIDENTIAL CLIENT DOCUMENT · 2026

security@mandatemind.com · 502-509-7737 · mandatemind.com/security

MandateMind Security & Data Protection

MandateMind AI is a cloud-based Governance, Risk, and Compliance (GRC) platform designed to help organizations maintain real-time alignment between mandates, controls, and evidence.

This document provides a transparent overview of:

- What data MandateMind collects
- How data enters the platform
- How data is stored and encrypted
- How data is processed
- How tenant isolation works
- How long data is retained
- Our compliance posture
- Our subprocessors and security controls

MandateMind does **not** scan cloud environments, ingest logs, or pull configuration data from client systems. All data is user-provided or platform-generated.

SECTION 1

What Data MandateMind Collects

MandateMind collects only the data required to operate the platform.

User-Provided Data

- Evidence files (PDFs, screenshots, policies, reports)
- Control responses
- Mandate mappings
- Assessment answers
- Notes, comments, remediation details

Identity & Account Data

- Name
- Email
- Role (Admin, Client, Auditor)
- Authentication metadata

Platform-Generated Metadata

- Evidence scoring metadata
- Drift detection metadata
- Control status metadata
- Audit logs
- System timestamps
- File integrity hashes

MandateMind Does NOT Collect

- ✗ Cloud configuration data
- ✗ Network logs
- ✗ Endpoint telemetry
- ✗ IAM policies
- ✗ Production system data
- ✗ Sensitive PII beyond user identity fields

SECTION 2

How Data Enters MandateMind

MandateMind supports three data entry paths:

Manual Uploads

Users upload evidence files directly through the UI.

Manual Input

Users enter control responses, mandate mappings, and remediation notes.

API (Optional)

Clients may use MandateMind's API to automate:

- Evidence uploads
- Control updates
- Mandate mappings

MandateMind does **not** automatically pull data from client systems.

SECTION 3

How Data Is Stored

MandateMind is hosted on Amazon Web Services (AWS) using industry-standard security practices.

Storage Architecture

Evidence	AWS S3
Application data	AWS RDS (PostgreSQL)
Logs	AWS CloudWatch
Backups	Encrypted S3 buckets

Encryption

In Transit	TLS 1.2+
At Rest	AES-256
Integrity	SHA-256 hashing

Tenant Isolation

MandateMind enforces strict logical separation:

- Tenant-scoped data boundaries
- Row-level access controls
- Segregated evidence storage paths
- RBAC enforcement

Tenants cannot access or view each other's data.

SECTION 4

How Data Is Processed

Evidence Processing

When evidence is uploaded:

- File is encrypted and stored
- Metadata is extracted
- Evidence is linked to a control
- Evidence scoring evaluates freshness and decay

Drift Detection

MandateMind analyzes:

- Control responses
- Evidence timestamps
- Mandate → control mappings

Drift is flagged when:

- Evidence is stale
- Controls lack coverage
- Mandates change
- Mappings are incomplete

AI Processing

MandateMind uses AI to:

- Summarize evidence
- Suggest mappings
- Highlight gaps
- Generate remediation guidance

AI models process only tenant-provided data. MandateMind does **not** use client data to train shared models.

SECTION 5

Access Controls & Security

RBAC Roles

Admin	Full tenant administration
Client	Standard user
Auditor	Read-only

Authentication

- Email + password
- Optional MFA
- Session expiration
- Device/session logging

Audit Logging

MandateMind logs:

- Logins
- Evidence uploads
- Control changes
- Mandate mappings
- Permission changes

Audit logs are immutable.

SECTION 6

Subprocessors

MandateMind uses the following subprocessors:

Amazon Web Services (AWS)	Hosting, storage, compute
Azure OpenAI / OpenAI	AI processing (no training on client data)
Cloudflare	CDN, DDoS protection
SendGrid	Transactional email

A full subprocessor list is maintained at: **mandatemind.com/subprocessors**

SECTION 7

Data Residency

All customer data is stored in **United States AWS regions** (default). Additional regions may be added based on demand.

SECTION 8

Data Retention & Deletion

Retention

Evidence files	Retained until deleted by the tenant
Audit logs	90 days by default
Backups	30 days

Deletion

Upon tenant request:

- Evidence files are permanently deleted
- Database records are purged
- Backups age out automatically

MandateMind does not retain client data after contract termination.

SECTION 9

Compliance Posture

MandateMind aligns with:

SOC 2	**ISO 27001**	**NIST**	**PCI DSS**	**HIPAA**

MandateMind is actively pursuing **SOC 2 Type II** certification.

Contact & Support

For security or data handling questions:

security@mandatemind.com
support@mandatemind.com

502-509-7737 · mandatemind.com/security