

# **Security and Compliance Handbook**



## What Is Material Model?

Material Model automates time-and-motion study analysis from video (recorded by hand-held, body-worn, or fixed cameras). We produce a structured element breakdown and work-step timing and common statistical analysis in our web-based portal, with export to CSV. Customers use our service to improve industrial ergonomics, maintain safety, keep routings current and support audits. Our software is hardware agnostic and can be used without any new hardware install and works alongside your MES.

## Our commitment to security

### **At Material Model, customer trust is our #1 priority.**

Our customers trust us with the video data of their most proprietary processes. Our security practices are centered on making sure this trust is earned. We treat all customer videos, documents, and derived data as sensitive, and operate a defense-in-depth architecture: strict authentication and role-based access, input validation, private-networked data stores, encryption in transit and at rest, least-privilege identities, audit logging, and monitored infrastructure.

### **We work hard to make sure your IT department can rest easy.**

We collaborate closely with your security team from day one. We align to your vendor review process, provide clear architecture and data-flow documentation, and support SSO, least-privilege access, and auditable activity logs. We sign the right agreements (e.g., NDA/BAA as needed), honor documented retention controls, and give named points of contact and change notifications for anything that could affect your environment.

# Enterprise Security

## Data Encryption

We secure data end-to-end. All application traffic is served over TLS, and stored data is encrypted at rest with AES-256. That covers source videos, structured outputs, and operational metadata.

## Principle of Least Privilege

Access is provisioned on least privilege. Roles are scoped so users only see what they need to do their work. All actions are logged and fully auditable.

## Data Retention

We keep data available and recoverable. By default, backups run daily and are retained for 14 days. For enterprise customers, we can setup custom data retention policies, including separate retention for video data, structured outputs, and metadata.

## Data Governance

We have robust security policies to ensure data availability and proper handling in accordance with industry best practices.

## Private VPC

Our storage and video-processing services run on private VPC infrastructure, ensuring your data is isolated from public networks and protected by enterprise-grade security controls.

## Built on Google Cloud Platform

Material Model is built on the GCP cloud platform, which provides 99.99% availability across multiple US regions.

## Multi-Factor Authentication (MFA)

MFA is mandatory for all sensitive operations, providing extra security controls to prevent unauthorized access.

## Third Party Data Processors

Material Model uses third party LLM providers Google, OpenAI, and Anthropic for some of its AI features. We have carefully chosen these providers based on their security measures and adherence to enterprise-grade security compliance standards.

### Zero Data Retention

Material Model has Zero Data Retention (ZDR) agreements with our AI providers Gemini, OpenAI, and Anthropic. This means your uploaded videos and analyzed data are **never** stored beyond their AI processing. All information processed is deleted instantly. This ensures your data remains temporary and private.

### Secure AI Controls

Material Model's AI features use robust Role-Based Access Controls (RBAC) to regulate data access. All data is logically separated by customer ID, ensuring only authorized personnel and systems from your organization can access it.

### Monitoring and Auditing

Material Model monitors all third-party LLM interactions in real-time to detect anomalies and keep usage logs for auditing and transparency purposes.

### Encrypted Communications

All data exchanged between Material Model and the AI providers are encrypted in transit using industry-standard TLS protocols.

## Frequently Asked Questions

### **Does Material Model's retain a copy of my data?**

Yes. To ensure the highest-quality user experience, Material Model securely stores and encrypts uploaded videos and generated analyses for error monitoring, troubleshooting, and customer success purposes.

### **Can I request Material Model to delete my data?**

Yes. Please send an email to [security@materialmodel.com](mailto:security@materialmodel.com) and we will delete your data within 30 days.

### **Is Material Model's data securely stored?**

Yes. All data is encrypted in transit using TLS encryption and AES-256 bit encryption at rest, hosted on a private Google Cloud VPC with restricted access, secure private networks, and rotating IP addresses.

### **Do Material Model's 3rd party AI vendors save customer data?**

No. Material Model uses LLM providers to power its AI features - Google Gemini. Material Model has a ZDR (Zero Data Retention) agreement with our providers, meaning your data will not be logged, stored on their servers, or used for AI model training.

### **Does Material Model use my data for AI model training purposes?**

To ensure our models are continuously improving and at the bleeding edge, Material Model may leverage aggregated and anonymized usage patterns in our product development cycle. Enterprise users can opt out of this based on their specific data governance requirements. Please contact our team to discuss available data handling options for your organization.

### **How do you protect against malicious attacks against your AI models?**

Material Model protects AI models from malicious attacks through comprehensive input and output safeguards. We sanitize, validate, and monitor all inputs and outputs following security best practices, while continuously monitoring interactions and enforcing policy-based constraints.

## Get In Touch

Visit our website:

<http://www.materialmodel.com>

General inquiries:

[founders@materialmodel.com](mailto:founders@materialmodel.com)

Security questions:

[security@materialmodel.com](mailto:security@materialmodel.com)

Support requests:

[support@materialmodel.com](mailto:support@materialmodel.com)

Tel: 707-563-9099

### Mailing address

Material Model, Inc  
2261 Market Street STE 85311  
San Francisco, CA 94114

### Visit us

American Industrial Center  
2339 3rd St 3R #48  
San Francisco, CA 94158

