TRUST AND COMPLIANCE

How we handle client information

This document describes how Mayhem Shield handles client materials shared during implementation assurance engagements. It is written for security, privacy, legal, procurement, and approval stakeholders who need a clear picture of our practices before engagement starts.

Version 1.1 · Last reviewed April 2026 · Next review April 2027 or on material change

AT A GLANCE

Client materials are stored in Google Workspace (US region), encrypted client-side with XQ, accessed only from hardened founder endpoints with SSO and MFA. Default retention is 90 days after engagement close. All work is performed by the three Mayhem Shield founders, US-based, with no subcontractors. Confirmed security incidents affecting client materials are reported to affected clients within 48 hours.

1. Purpose and scope

Mayhem Shield conducts buyer-side implementation assurance reviews of enterprise AI deployments. In the course of a review, clients share materials such as architecture diagrams, policy documents, configuration exports, screenshots, and interview notes. This document describes how those materials are handled from intake through destruction.

MATERIALS TYPICALLY RECEIVED

- Architecture and data-flow diagrams
- Policy and standards documents
- Configuration exports and screenshots
- Interview notes and meeting summaries
- System metadata (hostnames, APIs, regions, data classes)

MATERIALS NOT COLLECTED

- Production credentials, keys, or tokens
- Live customer or end-user data
- PII at scale or bulk personal records
- Source code access, unless explicitly scoped
- Administrative access to client systems

2. Legal entity and insurance

- **Entity:** Mayhem Shield, LLC (Texas, United States)
- **Professional liability (errors and omissions):** $5,000,000 per claim
- **Cyber liability:** $5,000,000 per claim

Certificates of insurance are available to clients on request.

3. Storage and infrastructure

- **Primary storage:** Google Workspace (Google Drive), US region.
- **Client-side encryption:** All client materials are encrypted locally with XQ before upload to Google Drive. Cleartext copies are not stored in Google Drive.
- **Endpoint security:** All founder workstations run Netskope for endpoint protection and data loss prevention. Workstations are hardened to a documented baseline including full disk encryption, automatic OS and application patching, screen lock enforcement, and restricted administrative access. Configuration

baseline available on request during procurement review.

- **Access control:** Single sign-on (SSO) is enforced on all accounts that access client materials. Multi-factor authentication (MFA) is required for all administrative and data-accessing actions.
- **Least privilege:** Access to engagement materials is limited to the founders assigned to that engagement. Founders not assigned to an engagement do not have routine access to its materials.
- **Controlled environment only:** Client materials are not copied to personal devices, consumer cloud storage, or non-enterprise tools. Material does not leave the controlled environment described above.

SUBPROCESSORS

PROVIDER	PURPOSE	DATA HANDLING POSTURE
Google Workspace Google LLC	Storage and collaboration for encrypted client materials	US region; standard enterprise data-processing terms
XQ Message XQ Message, Inc.	Client-side encryption before cloud upload	Keys controlled by Mayhem Shield; cleartext not held by subprocessor
Netskope Netskope, Inc.	Endpoint protection and data loss prevention	Telemetry only; no client materials processed in cleartext
Anthropic Anthropic PBC	AI analysis support via Claude for Work (Teams)	Customer data not used for model training under plan terms

4. Geographic operations

All three Mayhem Shield founders are United States based. Client materials are stored, accessed, and processed within the United States. Any travel with devices containing client materials is subject to the same endpoint security controls described in Section 3, and international transfer of client materials outside the United States requires prior written client approval.

5. AI tool usage disclosure

Mayhem Shield uses AI tools during engagement analysis and deliverable preparation. The following applies:

- **Tool in use:** Claude for Work (Teams plan) from Anthropic.
- **Training on data:** Under Anthropic's Claude for Work terms, customer data is not used to train Anthropic's models.
- **Other AI tools:** Client materials are not processed through consumer-tier AI products (for example, free-tier ChatGPT), unmanaged browser extensions, or any AI service without enterprise-grade data handling terms.

Clients who require that no AI tooling be used in their engagement can request this in writing before engagement start.

6. Retention and destruction

- **Default retention:** Engagement artifacts are retained for 90 days after engagement close.
- **Client-specified retention:** Where a client agreement specifies a different retention period (shorter or longer), the client agreement governs.
- **Destruction:** At the end of the retention period, artifacts are deleted from Google Drive and from any local or encrypted copies. Deletion is completed within 30 days of retention expiry.

- **Legal hold:** Retention may be extended beyond the default period where required by legal hold, regulatory investigation, client written instruction, or active dispute. Extended retention is documented in the engagement record.
- **Confirmation on request:** A written confirmation of destruction can be provided to clients on request.

7. Incident response

Mayhem Shield maintains an internal incident response process covering detection, containment, and client notification for security incidents involving client materials.

- **Notification window:** Clients will be notified within 48 hours of confirmed discovery of a security incident affecting their materials.
- **Scope of notification:** Notification will include the nature of the incident, the materials believed to be affected, containment steps taken, and expected next steps.
- **Post-incident reporting:** A written post-incident summary is provided to affected clients once the investigation is complete. Additional detail can be shared under NDA where appropriate.

8. Confidentiality and personnel

- **Non-disclosure agreements:** All three founders sign client NDAs as standard. Client-provided NDA templates are accepted; a Mayhem Shield mutual NDA is available if the client prefers.
- **No subcontractors:** All engagement work is performed by the three Mayhem Shield founders. No subcontractors, contractors, or offshore resources are engaged.
- **Independence:** Buyer-side reviews and vendor-side enablement are never combined on the same tool in the same engagement. Vendor relationships are disclosed before engagement.

9. Business continuity

In the event a founder assigned to an active engagement becomes unavailable, another founder may access engagement materials only with prior client notification, under the same SSO, MFA, and encryption controls described in Section 3. Access transitions are documented in the engagement record. No additional personnel are added to the engagement to preserve continuity.

10. Data processing agreements

Mayhem Shield does not maintain a standard DPA template at this time. We accept client-provided DPA templates and will negotiate terms to match client requirements. A standard Mayhem Shield DPA template is expected to be available in 2026.

11. Certifications and compliance posture

FIRM-LEVEL COMPLIANCE

- **SOC 2 Type II:** Engagement is planned for 2026–2027. Target observation period and auditor information available on request during procurement review.
- **Security questionnaires:** Completed CAIQ (Consensus Assessments Initiative Questionnaire) and SIG Lite responses available on request during procurement review.
- **Additional compliance documentation** (policies, control descriptions) can be provided on request during procurement review.

INDIVIDUAL CERTIFICATIONS

Held by the technical co-founders Tich Gandhe and Danny Hondo:

- CISM — Certified Information Security Manager (ISACA)
- CASP+ — CompTIA Advanced Security Practitioner
- AAIA — Advanced in AI Audit (ISACA)
- AAISM — Advanced in AI Security Management (ISACA)

Business and operations co-founder Cristina Lopes leads procurement documentation, compliance coordination, and client engagement operations. Role-specific credentials and background available on request during procurement review.

12. How to request additional documentation

Enterprise clients who need additional documentation during procurement review, including DPA negotiation, certificate of insurance, detailed security questionnaire responses, or reference checks, can contact:

- **Email:** info@mayhemshield.com
- **Primary point of contact:** Cristina Lopes, Co-Founder (Business and Operations Lead)

Standard turnaround for procurement documentation requests is three business days.

This document is reviewed annually or on material change to Mayhem Shield's practices, whichever is sooner. For the current version, contact info@mayhemshield.com.