How we handle client information

Mayhem Shield, LLC | Security and data handling | Version 1.2 | August 2026

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 data handling practices before engagement starts. The commitments below are reflected in our standard Data Processing Addendum, which is available on request.

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.

It covers personal data we process on a client's behalf. It does not cover ordinary business records where we act as an independent controller, such as contracting, billing, and business-contact data. Those are covered by our privacy notice.

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. Coverage statements describe the policies in force and are not guarantees of coverage or payment on any particular claim.

3. Roles and processing instructions

- **Our role:** For client materials, the client is the controller or business and Mayhem Shield is the processor or service provider. Where the client is itself a processor, we act as its subprocessor.
- **Documented instructions only:** We process client materials only on documented instructions, meaning the services agreement, the applicable order or statement of work, the Data Processing Addendum, and written instructions consistent with them.
- **No secondary use:** We do not sell or share client personal data, use it for advertising, use it for unrelated commercial purposes, or retain, use, or disclose it outside the direct business relationship with the client.
- **Unlawful instructions:** If we believe an instruction conflicts with data protection law, we tell the client and may suspend the affected processing until the question is resolved.

4. Storage and infrastructure

- **Primary storage:** Google Workspace (Enterprise edition), Google Drive. A US data region policy is applied to data at rest for covered Workspace services.
- **Encryption:** Data is encrypted in transit and at rest. Client materials are additionally 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, with full disk encryption enforced.
- **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. Access follows least-privilege principles, is reviewed periodically, and is revoked promptly when no longer required.
- **No shared credentials:** Shared credentials are prohibited, and client credentials are not stored in deliverables or working notes.
- **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.
- **Secure transfer:** Materials are exchanged through agreed business channels. Highly sensitive evidence uses a secure transfer method agreed with the client before the transfer.

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 (Team plan) from Anthropic. This is the only authorized external generative AI service for engagement content unless a client approves another provider in writing.
- **Training on data:** Under Anthropic's Claude for Work terms, customer data is not used to train Anthropic's models. We do not use client personal data to train public, shared, or generalized models.
- **Client opt-out:** Clients may prohibit AI processing by written notice before the engagement begins or before the relevant material is submitted. The instruction is recorded and followed for the engagement, without reducing the contracted human review.
- **Human review:** Mayhem Shield personnel review material AI-assisted findings, severity determinations, recommendations, and deliverables before delivery. AI output is a drafting and analytical aid, not autonomous approval evidence.
- **Minimization:** Data minimization, redaction, or pseudonymization is applied where reasonably practicable, particularly for sensitive evidence.
- **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.

6. What we ask clients not to send

To keep the review scope proportionate, clients should not provide account passwords, private cryptographic keys, authentication tokens, full payment-card data, or unredacted government identifiers unless specifically required, approved in writing, and protected by additional agreed controls.

Protected health information requires an executed business associate agreement where HIPAA applies. Biometric data, children's data, and export-controlled material are out of scope unless expressly authorized in

the order with the applicable legal basis and safeguards identified.

7. Subprocessors and vendors

The following providers may process client materials used in an engagement:

- **Google Workspace (Google LLC):** business email and secure file storage. United States.
- **Anthropic, PBC:** enterprise AI-assisted analysis and drafting, limited to engagement content submitted under client instructions. United States. Clients may opt out before processing begins.

Vercel (website hosting and analytics) and Calendly (meeting scheduling, embedded on our contact page) support the website. They are not authorized to process engagement evidence, and their handling of ordinary website and business-contact data is covered by our privacy notice.

We give at least 30 days' notice before authorizing a new subprocessor that will process client materials, except where an emergency replacement is needed to maintain security or continuity. Clients may object in writing on reasonable data protection grounds during the notice period, and where no workable solution is available may terminate the affected services without penalty for the unperformed portion.

8. International transfers

Mayhem Shield is established in the United States, and processing takes place in the locations identified in our Data Processing Addendum. For transfers that require a mechanism under applicable law, our DPA incorporates:

- the EU Standard Contractual Clauses (Implementing Decision (EU) 2021/914), Module Two or Module Three as applicable, for EEA transfers;
- the current ICO International Data Transfer Addendum for UK transfers;
- the Swiss adaptations to the EU SCCs for transfers subject to the Swiss Federal Act on Data Protection.

We provide the information clients need for their transfer impact assessments on request. If we receive a binding government demand for client personal data, we notify the client unless legally prohibited, review the demand's legality, challenge overbroad or unlawful demands where reasonable, and disclose only what is legally required.

9. Incident response and breach notification

- **Notification target:** We notify the client without undue delay and, where feasible, within 48 hours of confirming a personal data breach affecting their data.
- **Contents:** The notice describes the nature of the incident, affected data and individuals, likely consequences, containment and remediation steps, relevant dates, and a contact for follow-up. Information is provided in phases as it becomes available rather than held back pending a complete investigation.
- **Regulator and individual notice:** We do not notify regulators or affected individuals on a client's behalf unless instructed, legally required, or immediate notice is necessary to prevent material harm.
- **What is not a breach:** Unsuccessful attempts, routine scanning, and blocked attacks that do not compromise client data are not treated as personal data breaches, though related evidence is available through the audit process where reasonably necessary.

10. Retention, return, 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.
- **Return or deletion:** At termination, clients may elect return of their materials in a reasonably usable format, deletion, or both, unless law requires retention. Absent an election, our documented retention schedule applies.
- **Destruction:** At the end of the retention period, artifacts are deleted from Google Drive and from any local or encrypted copies within 30 days. Data held in provider-managed backups is isolated from ordinary use and ages out through the provider's normal backup lifecycle.
- **Confirmation on request:** A written confirmation of destruction can be provided to clients on request.

11. Individual rights and regulatory assistance

If we receive a request from an individual about data we process for a client, we notify the client promptly and do not respond substantively except on the client's instruction or where legally required. We provide reasonable assistance so the client can respond to access, correction, deletion, portability, restriction, objection, and opt-out requests.

We also assist with data protection impact assessments, prior consultations, and regulator inquiries, and we inform clients promptly of any regulator inquiry specifically concerning their data unless prohibited. Our assurance work and this assistance are not legal advice and are not a certification of any client's compliance.

12. Audit and evidence

We make available the information reasonably necessary to demonstrate compliance with our data protection commitments, including security documentation, relevant policies, completed questionnaires, third-party reports where available, and remediation status.

Clients ordinarily rely on that evidence and remote review first. Where it is insufficient, a client may conduct one audit per 12-month period, itself or through an independent auditor bound by confidentiality, on at least 30 days' notice. A confirmed breach, a regulator request, or credible evidence of material noncompliance justifies a more urgent or additional audit. Audits exclude access to systems and data belonging to other clients.

13. 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 consulting subcontractors or offshore resources process engagement materials unless disclosed and authorized in advance under the subprocessor terms above.
- **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.

- **Survival:** Confidentiality obligations continue for as long as we hold client materials and thereafter as required by the client agreement and law.

14. Data processing agreement

A standard Mayhem Shield Data Processing Addendum is available on request. It covers the commitments described on this page, including processing roles and instructions, the AI processing terms and opt-out, subprocessors, international transfer mechanisms, breach notification, retention and deletion, individual rights assistance, and audit rights.

Client-provided DPA templates are also accepted, and we will negotiate terms to match client requirements. Where a client is subject to HIPAA, a business associate agreement is executed before any protected health information is received.

15. Certifications and compliance posture

Individual certifications

Held by the technical co-founders Tich Kadandara 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)

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.
- Additional compliance documentation (policies, control descriptions) can be provided on request during procurement review.

16. How to request additional documentation

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

- **Email:** info@mayhemshield.com
- **Phone:** (469) 237-8537
- **Primary point of contact:** Tich Kadandara, tkadandara@mayhemshield.com

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.