Mabble Helix - HECVAT-Lite Pre-Filled Responses

This document holds Mabble's responses to the EDUCAUSE Higher Education Community Vendor Assessment Toolkit - Lite (HECVAT-Lite) v3. HECVAT is the standard TPRM artefact requested by United States colleges and universities under FERPA, GLBA, and state research-data laws.

Scope caveat. As of 2026-05-14, Mabble Helix has not signed a higher-education design partner. The product is positioned for healthcare and patient-data use cases first. Many HECVAT-specific questions therefore answer **"Not applicable - no higher-education vertical in current scope"** until the first edu design partner is signed.

The answers reflect the core HIPAA-grade platform that would underlie any future edu deployment. Where the same control is already enumerated in the CAIQ pack, the Evidence column cross-references it.

---

1. Company Overview

ID	Question	Answer	Notes
1.1	Company legal name	Mabble, Inc. (doing business as "Helix")	Delaware C-corporation
1.2	Primary product or service offered	Mabble Helix - HIPAA-grade vault platform for sensitive personal data	See `internal/research/20_helix_inventory.md`
1.3	Year founded	2025	
1.4	Number of employees	Pre-launch, small team	Specific headcount available under NDA
1.5	Annual revenue	Pre-launch	Specific figures available under NDA
1.6	Subsidiaries / parent organisations	None	Standalone Delaware C-corp
1.7	Primary contact for security inquiries	Compliance Office	sales@mabble.ai
1.8	Primary contact for privacy inquiries	Compliance Office	sales@mabble.ai

---

2. Documentation

ID	Question	Answer	Notes

2.1	SOC 2 Type II report	Not yet issued	Planned for the 6-month launch window. See `internal/compliance/README.md §5`.
2.2	SOC 2 Type I report	Not yet issued	Same window as Type II.
2.3	ISO 27001 certification	Not held	Not pursued in the current phase.
2.4	HITRUST CSF certification	Not held	Not pursued.
2.5	PCI-DSS Attestation of Compliance	N/A	Helix does not process card data; billing is delegated.
2.6	Most recent penetration test report	Not yet issued	External pen test engagement pending.
2.7	Most recent vulnerability scan report	Available under NDA	Container image scanning (Trivy or equivalent) on every CI build.
2.8	Cyber-insurance certificate	Manual attestation required	Mabble engineering / Finance attestation needed before disclosure.
2.9	Privacy Policy URL	Public-facing on the marketing site	See Phase 2 Privacy Notice with version history.
2.10	Sub-processor list	Public	`docs/compliance/sub_processors.md` and `internal/compliance/vendor_risk_matrix.md`.

3. Company Information

ID	Question	Answer	Notes
3.1	Does your company have a documented information security programme?	Partial	See CAIQ GRM-01. Mabble engineering Gauntlet is the most recent formal risk assessment.
3.2	Does the information security programme address the CIA triad (Confidentiality, Integrity, Availability)?	Yes	Encryption (C), audit-log Merkle chain + AES-GCM authenticated encryption (I), Multi-AZ + SLO/SLI + alerting (A).
3.3	Is a Chief Information Security Officer (CISO) or equivalent appointed?	Partial	Mabble engineering is the executive owner of information security. Dedicated CISO is on the post-launch hiring plan.
3.4	Are employees subject to background checks?	Manual attestation required	HR-controlled. See SIG-Lite Q.1.1.
3.5	Is security awareness training provided to employees?	Partial	Onboarding training present; annual refresher is a roadmap item.

4. Application / Service Security

ID	Question	Answer	Notes
4.1	Does your application authenticate users via federation (SAML 2.0, OIDC, Shibboleth, CAS)?	Yes - SAML 2.0 and OIDC supported. Shibboleth is interoperable via SAML 2.0. CAS is not directly supported; would require a SAML adapter.	See CAIQ IAM-11.
4.2	Does your application support SCIM 2.0 for provisioning?	Yes	See CAIQ IAM-11.
4.3	Does your application support multi-factor authentication (MFA)?	Yes	WebAuthn passkey preferred; TOTP fallback. AMR tagging on every session. See CAIQ IAM-01.
4.4	Does your application support InCommon federation?	Partial	SAML 2.0 metadata is exportable; InCommon-specific attribute mapping is supported on configuration. No production deployment with an InCommon IdP yet.
4.5	Are authentication credentials encrypted in storage?	Yes	Argon2id password hashing; WebAuthn public-key registration; TOTP secrets envelope-encrypted at rest. See CAIQ IAM-05.
4.6	Are session tokens scoped per user and per service?	Yes	Capability tokens, server-side only, scoped per RPC. No long-lived broad tokens. See CAIQ IAM-12.
4.7	Does your application support row-level multi-tenancy isolation?	Yes	PostgreSQL RLS + FORCE RLS on every PII-bearing table; per-tenant DEK pool. See CAIQ IVS-02.
4.8	Is data encrypted at rest?	Yes	AES-256-GCM per record plus AWS-managed disk encryption underneath. See CAIQ EKM-01.
4.9	Is data encrypted in transit?	Yes	TLS 1.3. See CAIQ EKM-03.
4.10	Is the application subject to a documented Secure SDLC?	Yes	OWASP ASVS Level 2 informs the test plan; mandatory code review; SAST on every build. See CAIQ AIS-01.

5. Higher-Education Vertical Questions

These questions apply only where Mabble Helix is providing services to a higher-education institution. As of 2026-05-14, no higher-education design partner is contracted; the responses below reflect the platform's readiness rather than a live deployment.

ID	Question	Answer	Notes
5.1	Will the service process FERPA-covered student records?	Not applicable today	No higher-education vertical in current scope. Should an institution onboard, FERPA School Official Exception status would be invoked (34 CFR §99.31(a)(1)); the customer remains the data steward, Helix is the processor.
5.2	Will the service process research data subject to HIPAA / FDA / 21 CFR Part 11?	Conditionally yes	Helix's HIPAA-grade controls apply unchanged. 21 CFR Part 11 (electronic signatures) audit-trail requirements map onto the existing Merkle-anchored audit log; explicit Part 11 attestation is a roadmap item.
5.3	Will the service process data subject to GLBA (financial aid)?	Not applicable today	No higher-education vertical in current scope.
5.4	Does the service support integration with Student Information Systems (Banner, Workday Student, PeopleSoft)?	Not applicable today	Integration would require a customer-specific connector; not on the current roadmap.
5.5	Does the service support integration with Learning Management Systems (Canvas, Blackboard, Brightspace)?	Not applicable today	Same as 5.4.
5.6	Will the service process directory-information records under FERPA §99.37?	Not applicable today	No higher-education vertical in current scope.
5.7	Will the service process special-category research data (e.g., human-subject genomic data)?	Conditionally yes	Special-category lawful-basis flag (GDPR Art. 9) is supported in the lawful-basis tagging system; jurisdiction tagging supports US-state-specific genomic-data laws. Customer-specific data dictionary required at onboarding.

6. Datacenter and Hosting

ID	Question	Answer	Notes
6.1	Where is the data hosted (geographic region)?	AWS us-east-1 by default. AWS eu-west-1 available on request for EU-residency customers.	Per-tenant Data Residency Registry (DRS, R-P1.22).
6.2	Is the hosting provider certified (SOC 2, ISO 27001, FedRAMP)?	Yes - AWS	AWS SOC 2 Type II, ISO 27001, FedRAMP Moderate (where applicable).
6.3	Are physical security controls documented?	Yes - by AWS	See CAIQ DCS series.
6.4	Is data physically segregated from other customers?	Logical via RLS + per-tenant DEK pool	See CAIQ IVS-02.
6.5	Are backups encrypted?	Yes	AWS RDS encrypted snapshots + S3 SSE-KMS.

---

7. Privacy

ID	Question	Answer	Notes
7.1	Is the service compliant with FERPA where applicable?	Conditionally yes	Helix would operate under the FERPA School Official Exception (34 CFR §99.31(a)(1)) where contracted with an institution. No data sharing outside the institution's authorisation.
7.2	Is the service compliant with GDPR for EU students / staff?	Yes - as Processor	EU SCC Module 2 supported. See `internal/compliance/SCC_module_2_cover_letter.md`.
7.3	Is the service compliant with CCPA / CPRA for California students?	Yes - as Service Provider	See SIG-Lite N.1.8.
7.4	Is the service compliant with state student-data-privacy laws (e.g., SOPIPA, NY Ed Law §2-d)?	Conditionally yes	Helix's existing controls (no advertising-based monetisation, no targeted advertising, no sale of data, jurisdiction tagging, audit logs) match the substantive requirements of SOPIPA and NY Ed Law §2-d. Specific contractual riders required at onboarding.

7.5	Is a Data Protection Officer appointed?	Partial - interim	Compliance Office serves as interim DPO contact. See SIG-Lite P.1.4.
7.6	Are data subject rights (access, correction, deletion) supported?	Yes	DSAR workflow (Phase 1-1.7). See CAIQ IPY-03.
7.7	Is consent collected where required?	Yes	CMP with consent receipts, GPC, 13-month TTL (Phase 3). See SIG-Lite P.1.2.
7.8	Are records of processing activities (ROPA) maintained?	Yes	ROPA Art. 30 (Phase 4).
7.9	Will student or research data be used for any secondary purpose (e.g., training AI models)?	No	All processing is bound to the lawful basis and purpose of use declared per record. Use of customer data to train models is contractually prohibited (BAA §3 and DPA Art. 28(3)(a)).

---

8. Vulnerability Management

ID	Question	Answer	Notes
8.1	Are vulnerability scans performed regularly?	Partial	Container image scanning on every CI build; network-tier external scanning is on the roadmap. See CAIQ IVS-05.
8.2	Are patches applied within a defined SLA?	Yes	Critical 7 days / high 30 / medium 90 / low next release. See CAIQ TVM-02.
8.3	Is a vulnerability disclosure programme in place?	No	Draft VDP exists; not yet live. See CAIQ TVM-03.
8.4	Are penetration tests performed at least annually?	No	Not yet engaged. See CAIQ IVS-06.

---

9. Incident Management

ID	Question	Answer	Notes
9.1	Is a documented incident response plan in place?	Yes	See CAIQ SEF-01.

9.2	What is the notification commitment for confirmed data breaches?	<=30 calendar days under the BAA; <=72 hours to a GDPR supervisory authority under Art. 33; without undue delay to data subjects under Art. 34.	See `internal/compliance/breach_notification_runbook.md`.
9.3	Are FERPA-applicable incidents reported in line with institutional policies?	Conditionally yes	Helix follows the customer's institutional incident-reporting timing where stricter than the BAA default.
9.4	Is forensic data preserved for incident investigation?	Yes - audit log	RFC 6962 Merkle chain plus Sigstore Rekor external anchor (D-005). See CAIQ SEF-04.

---

10. Termination

ID	Question	Answer	Notes
10.1	Is customer data returned or destroyed on contract termination?	Yes	Per BAA §11 and DPA template - at customer's option. See CAIQ IPY-04.
10.2	What is the maximum window for return / destruction?	30 days for production data; 90 days residual in encrypted backups before crypto-shred completes.	Disclosed in BAA §11.3.1.
10.3	Is a certificate of destruction issued?	Yes - on customer request	Signed attestation from the Compliance Office.

Summary statistics

Section	Total	Yes	Partial	No	N/A	Manual Attestation
1 - Company Overview	8	8	0	0	0	0
2 - Documentation	10	1	1	7	1	1 (cyber insurance)
3 - Company Information	5	1	3	0	0	1
4 - Application Security	10	9	1	0	0	0
5 - Higher-Ed Vertical	7	0	2 (conditional)	0	5	0

6 - Datacenter and Hosting	5	5	0	0	0	0
7 - Privacy	9	7 (incl. conditional)	2	1	0	0
8 - Vulnerability Management	4	1	1	2	0	0
9 - Incident Management	4	4 (incl. conditional)	0	0	0	0
10 - Termination	3	3	0	0	0	0
Total	**65**	**39**	**10**	**10**	**6**	**2**

(Section 1 contains administrative facts rather than control answers; counts above include them for completeness. Manual attestation count = Mabble engineering / Finance attestation required before submission.)

Change log

Version	Date	Change
0.1.0	2026-05-14	Initial Track C publication.