

MTestHub Security & Privacy Overview

MTestHub, Inc., a Delaware corporation (United States of America) · Generated October 24, 2026 · Trust Center last updated October 22, 2026

This overview is generated automatically from MTestHub's approved Trust Center registry. It contains only statements that are currently approved for publication; items that are not yet complete are labelled as In Progress, Planned or Being Confirmed. It is informational and does not replace a signed agreement or DPA.

Compliance status

Framework	Status	Statement
SOC 2	In Progress	SOC 2 Readiness Program Underway. MTestHub is actively building and documenting its security-control environment in alignment with the AICPA Trust Services Criteria as part of its SOC 2 readiness program. No SOC 2 examination has been completed yet. We will update this Trust Center as formal audit milestones are completed.
UAE PDPL	In Progress	UAE PDPL Readiness. MTestHub is reviewing its practices against the UAE Personal Data Protection Law (Federal Decree-Law 45/2021). Final legal review is pending.
ISO/IEC 27001	Planned	ISO/IEC 27001 — Not Certified. MTestHub is not ISO/IEC 27001 certified.
HIPAA	Not Applicable	HIPAA — Not Applicable. MTestHub is a recruiting platform and is not designed to process protected health information (PHI). Do not upload PHI.

Security controls

Control	Status	Description
Encryption in Transit	Implemented	The application and API are served over HTTPS (TLS). Session cookies are marked Secure.
Encryption at Rest	Being Confirmed	Database and file storage encryption at rest is provided at the hosting layer; details are being confirmed with our infrastructure provider before we publish specifics.
Authentication	Implemented	Passwords are hashed with PBKDF2-SHA256 (200,000 iterations, per-user salt). Sessions use httpOnly, Secure, SameSite cookies. Google sign-in is supported. Email verification is required for new accounts.
Abuse Protection	Implemented	Login, application, upload and other public endpoints are rate-limited.
Role-Based Access Control	Implemented	Organization roles (Owner, Admin, Recruiter, Hiring Manager, Interviewer, Viewer) and permission settings restrict who can view, export or act on candidate data. Internal MTestHub staff roles are separate and least-privilege.
Multi-Tenant Isolation	Implemented	Every customer record is scoped to its organization; APIs only return data for the signed-in organization. Candidates' applications are never shared with other employers.
Support Access	Implemented	MTestHub staff access to a customer workspace requires an authorized support session with a reason, is time-limited, visibly bannered and audit-logged.
Audit Logging	Implemented	Security-relevant actions — sign-ins, role and permission changes, exports, deletions, settings changes, support access — are recorded in an audit log available to organization administrators.
Secrets Management	Implemented	Credentials and API keys are stored as environment secrets, never in source code or client bundles.
Secure File Handling	Implemented	Uploads are checked for type, size and file signature; documents are parsed as data only — macros and embedded scripts are never executed.
Error & Performance Monitoring	Implemented	Application errors, latency and failed requests are monitored and grouped into issues for triage.

Control	Status	Description
Data Deletion & Export	Implemented	Organizations can export data and configure retention. Candidates can withdraw and request deletion from their portal.
Backups & Recovery	Being Confirmed	Backup frequency, retention and restore testing are being documented. We do not publish RPO/RTO targets until they are defined and tested.
Vulnerability Management	In Progress	Dependency updates and security reviews are performed as part of development. A formal vulnerability-management program is being documented.
Penetration Testing	Planned	An independent penetration test has not yet been completed.
Secure Development	In Progress	Code review, automated tests and type-checking run before release. Formal SDLC policy documentation is in progress.
Incident Response	In Progress	Incidents are tracked internally with severity, containment, investigation, notification assessment and post-mortem. Notification follows the obligations of the applicable law and contract.
Business Continuity	Planned	A business continuity and disaster recovery plan is being defined.
Vendor Risk Management	In Progress	Subprocessors are tracked in a registry with purpose, data categories, DPA status and review dates.
Enterprise SSO (SAML)	Planned	SAML SSO for enterprise identity providers is planned.

AI & responsible hiring

AI extracts job-related evidence and recommends validation; people make every hiring decision. MTestHub does not infer protected characteristics, score appearance, emotions, voice or accent, or automatically reject candidates.

AI data training: Customer and candidate data is not used to train general-purpose AI models. AI providers process data only to return results to MTestHub.

Data hosting & transfers

Primary hosting region and subprocessor locations are being confirmed with our infrastructure providers. We do not currently offer contractual data residency.

Data retention & deletion

Customers configure retention for candidate data (default 730 days) and video/audio (default 90 days). Customers can export and delete data; candidates can request deletion. Backups may retain copies temporarily until they expire on their normal lifecycle.

Subprocessors

Provider	Purpose	Data categories	Location
Emergent Labs	Application hosting, database hosting and deployment platform; AI model gateway; managed email delivery and Google sign-in integration	All customer and candidate data processed by the service	To be confirmed
Anthropic (via Emergent AI gateway)	AI language-model processing for screening, job and assessment generation, summaries and copilot	Redacted résumé text, job criteria, assessment responses, recruiter prompts	To be confirmed
Resend (via Emergent)	Transactional email delivery	Recipient name and email address, email content	To be confirmed
Stripe	Subscription billing and payment processing	Billing contact, company details, payment metadata (card data handled by Stripe, not stored by MTestHub)	To be confirmed

Provider	Purpose	Data categories	Location
Google (OAuth sign-in)	Optional 'Continue with Google' authentication	Name, email address, profile image of users who choose Google sign-in	To be confirmed
AssemblyAI	Speech-to-text transcription of video/audio assessment responses (only when enabled)	Candidate audio/video recordings and transcripts	To be confirmed

Documents

Document	Access	Status
Privacy Policy (v1.0)	Public	Available
Candidate Privacy Notice (v1.0)	Public	Available
Terms of Service (v1.0)	Public	Available
Acceptable Use Policy (v1.0)	Public	Available
Data Processing Addendum (v1.0)	Public	Available
Subprocessor List (v1.0)	Public	Available
Cookie Policy (v1.0)	Public	Available
Security Overview (v1.0)	Public	Available

Contact

Security: contact@mtesthub.com · Privacy: contact@mtesthub.com · Trust Center: <https://app.mtesthub.ae/trust>