

Enterprise Security & Compliance Whitepaper

Version 1.0 · October 2026 · www.hrmbt.com

1. Executive summary

MBT — Much Before Transformation — is an enterprise SaaS platform for evidence-first, vendor-neutral organisational and HR transformation research. Organisations use it to trace problems to their real causes and to set direction for both business and technology roadmaps.

Because customers bring sensitive organisational context into MBT, security is designed into the platform rather than added later. This whitepaper describes, in plain language, the controls that exist today, how customer data is separated and handled, and our honest position on formal certification.

2. Security principles

- Least access: every user is verified and approved before they can sign in.
- Separation by default: each organisation's data is isolated from every other organisation's.
- Your documents stay yours: uploaded workspace documents are never sent to public research engines and never used to train AI models.
- Server-side enforcement: permissions are checked on the server and in the database, never only by hiding buttons.
- Honest disclosure: we state only what is implemented and say clearly what is not.

3. Identity and access control

- Sign-in restricted to verified business email addresses; personal mailboxes are rejected on the server.
- Single-use, time-limited sign-in codes delivered by email, with per-email and per-network rate limits.
- Administrator approval required before first use; administrators can revoke access at any time.
- Three usage levels assigned by administrators; administrative roles are stored separately from user profiles and verified on the server.

4. Tenant isolation

Every research session, report, uploaded file and account record is tied to its owner. Access is enforced by row-level database policies and server-side authorisation for both interface and direct requests, so one customer cannot reach another customer's research, files or outputs by changing an identifier.

5. Bring-your-own-documents (BYOD)

- Uploaded files are held in private storage that is not publicly reachable; downloads use time-limited signed links.
- Document text is indexed into passages tagged to your organisation and separated at the database level.
- Every upload and written input is checked for relevance against your locked research scope before it is indexed or used.

- Workspace documents are used only for your own analysis and are never passed to public research engines.
- Deleting a file, or purging the workspace, permanently removes the file and every passage derived from it.

6. Zero-retention research mode

Each research run can be performed in zero-retention mode. Findings are held privately only while the run is open and are permanently deleted when the tab is closed, the user signs out or a new study starts; any residue is swept within 24 hours. Anything the user wants to keep must be exported first.

7. AI governance

- We do not use customer inputs, saved sessions or uploaded documents to train our own models, and we never sell them.
- AI and research providers receive only the text needed to produce the requested output, under their own terms.
- All external and user-supplied text is fenced as untrusted content before reaching a reasoning model, to reduce prompt-injection risk.
- Proprietary prompts, taxonomy and scoring logic run only on the server and are never shipped to the browser.
- Research calls run at temperature zero, and every output carries a run identifier and valid-as-of date for traceability.
- Every claim is labelled FACT, EVIDENCE, INFERENCE or HYPOTHESIS; sources are never fabricated.

8. Infrastructure and data location

- Standard workspace: account records, saved research and workspace documents are held in managed cloud infrastructure in Asia Pacific (Singapore).
- The website is delivered through a global edge network that passes data through in transit but stores none.
- Transport encryption is used for all traffic; at-rest protection is provided by the managed cloud infrastructure.
- Dedicated regional workspaces — EU (Frankfurt), UK (London), North America (Virginia), India (Mumbai), GCC (UAE / Bahrain) or Australia (Sydney) — are available on request, agreed case by case and confirmed in a Data Protection Addendum.

9. Operational security

- Audit logging of access and administrative actions.
- Rate limiting on authentication and AI endpoints.
- Security response headers and a content security policy.
- Secrets held only on the server, never in the browser.
- Consent records and governance registers maintained for review.

10. Compliance position and roadmap

MBT does not currently hold SOC 2, ISO/IEC 27001 or any equivalent certification, and has not published an independent penetration test. Our controls are designed with the ISO/IEC 27001 and SOC 2 Trust Services Criteria in mind.

Planned next steps, prioritised as enterprise customers require them: a documented information security management system and policies, an independent penetration test, SOC 2 Type I followed

by Type II, and ISO/IEC 27001 where customers need it. We will not display any certification mark until an accredited auditor has issued it.

11. Security contact and further information

Security questions, vulnerability reports and procurement questionnaires can be sent to the contact address on our Data & Security page. Under NDA we can share additional detail for enterprise security reviews.