

| Assess & Connect Technical FAQ's

Thomas' information security is outlined in **TT II_Information & Data Security at Thomas**, these FAQs provide supplementary documentation. Should you still have any outstanding queries, please direct them to your account representative.

Scope

Where 'Thomas' or 'Thomas International' is referred to within this document, we include any subsidiary of TIQ Topco Ltd. Specifically our trading businesses in the UK, France, Belgium, The Netherlands, South Africa, and Australia.

Table of Contents

1. Data Protection.....	2
2. Hosting, Residency & Sub-processors.....	2
3. Human Resources	3
4. Physical Security.....	4
5. Access, Authentication & Authorisation.....	4
6. Encryption & Key Management.....	4
7. Network, Edge & Platform Security.....	5
8. Secure Development & Change	5
9. Business Continuity, Backup & Recovery	5
10. Vulnerability Management & Penetration Testing	6
11. Data Separation, Retention & Deletion	6
12. Incident Response & Client Notification	6
13. Artificial Intelligence (AI), Automation & Responsible Use.....	7

1. Data Protection

Q) Who is the formally appointed Data Protection Officer (DPO) at Thomas?

A) The DPO function is fulfilled by Thomas' General Counsel. Contact: gdpr@thomas.co.uk

Q) Do you transfer personal data provided to any countries outside of the EEA, e.g. when you are using external Data Centres or Cloud Systems?

A) No – Thomas uses the MS Azure within the EEA.

Q) Do you comply with all applicable laws and regulations when dealing with an individual's personal identifiable information, particularly those relating to the General Data Protection Regulation ("the GDPR") and Data Protection Act 2018 ("the DPA")?

A) Yes. Thomas operates an established privacy and security framework aligned to GDPR, UK DPA 2018, and applicable regional laws. Privacy notices: [Privacy Notices | Thomas.co](#)

Q) Who in Thomas is responsible for the day-to-day security?

A) Day-to-day information security is managed by Platform Engineering and Security in partnership with Legal, with senior oversight.

2. Hosting, Residency & Sub-processors

Q) Where is Assess & Connect hosted?

A) Assess and Connect are hosted in Microsoft Azure – West Europe (Netherlands), with secondary recovery in North Europe (Ireland).

Q) Do you transfer personal data outside the UK/EEA?

A) Production hosting is within the EEA. Where cross-border transfers occur (e.g., support tooling or integrations), Thomas uses approved safeguards such as Standard Contractual Clauses.

Q) Which sub-processors do you use?

A) Key platform sub-processors include Microsoft Azure (compute, storage, databases, monitoring) and Cloudflare (WAF / edge security). Full list of sub processors here – [Privacy Notices | Thomas.co](#)

Azure maintains certifications such as ISO 27001 and SOC 1/2/3; details are available via [Microsoft's Service Trust Portal](#).

3. Human Resources

Q) Please provide details of the background checks (including DBS) your organisation carries out on potential staff or contractors.

A) Thomas ensure DBS checks are undertaken when deemed necessary. Thomas occasionally works in the education sector and for any staff involved DBS checks are undertaken as standard.

Q) What steps do Thomas take to check the previous employment history and experience of candidates for vacancies within Thomas, including resolving any gaps, discrepancies, or anomalies in their employment history?

A) Thomas takes up references and have a robust recruitment process in place to ensure we recruit and retain the right people for internal roles.

Q) Please confirm your recruitment processes include obtaining independent professional references that answer specific questions to help assess an applicant's suitability for the role.

A) Yes

Q) Do references need to be obtained prior to the potential employee starting with the company?

A) Yes

Q) Please state whether your organisation has adopted an Information Security and Acceptable Use Policy (including IT assets) and whether this forms part of an employee's terms of employment.

A) Yes. The organisation has formally adopted a comprehensive Information Security Policy and an Acceptable Use of Technology and Workspace Policy, which together govern the secure and appropriate use of information, systems, and IT assets across the business. These are incorporated into Thomas' employment contracts and Staff Handbook.

Q) How do you manage access during employee lifecycle changes?

A) Structured Starters-Movers-Leavers processes ensure prompt provisioning, change and revocation of access.

Q) Please describe how you ensure users only have access to the data they need (E.g. how you prevent privilege creep etc.).

A) Thomas undertakes regular reviews of Access Rights and any elevation rights is subject to an approval process

Q) Please provide details of the mandatory information security or data protection training your company provides to its staff and the frequency this is required to be refreshed.

A) All staff (both temporary and permanent) undertake mandatory online training for IT Security and GDPR (Data Protection).

4. Physical Security

Q) Is the site protected by 24-hour security? If so, please state the particulars of this (E.g. CCTV, guard services etc.).

A) Yes, Thomas uses MS Azure Public Cloud with datacentres offering high levels of security including the use of measures including (but not limited to) access control, CCTV and 24-hour security guards. More information can be found [here](#).

Q) Do you operate a clear-desk policy?

A) Yes, clear desk and clear screen policies form a piece of our Acceptable Use of Technology and Workspace Policy.

5. Access, Authentication & Authorisation

Q) How do users authenticate to Assess & Connect?

A) Username and password authentication, with a minimum password length of 12 characters and defined complexity requirements, or Single Sign-On (SSO) using Microsoft Entra ID / OIDC or SAML

Q) Is MFA supported or enforced?

A) Yes. MFA is supported and enforced through SSO providers

Q) How is least privilege enforced?

A) Least privilege is enforced through role-based access control (RBAC), using least-privilege defaults, plus periodic access reviews for elevated roles.

6. Encryption & Key Management

Q) Is data encrypted in transit and at rest?

A) Yes. TLS 1.2+ for data in transit; AES-256 for data at rest (including backups).

Q) How are encryption keys managed?

A) Keys and secrets are stored and managed in Azure Key Vault.

Q) Describe how data is protected internally within the service and how it's protected when being transferred on or using external networks.

A) Thomas ensure that LPA (least-privileged user account) is embedded in the role profiles and functions are segregated to ensure security. Thomas also follows the principle of Four Eyes in key decision making to ensure that no key decision is made by one person. Thomas also have IDS software and other technical measures in place to ensure the security of our data on our network, with system monitoring in place to ensure that should any suspicious activity be identified, Thomas IT are notified without undue delay and can take appropriate action.

7. Network, Edge & Platform Security

Q) How is the platform protected at the edge?

A) Cloudflare WAF with managed rules aligned to the OWASP Top 10 fronts public endpoints. Intra-service traffic is restricted within Azure virtual networks and service endpoints.

Q) Do you monitor and log activity?

A) Yes—centralised telemetry and alerting for availability, performance and anomalous events; security/audit logs of key actions are retained for ≥12 months.

Q) What measures do you take to protect the service against malware?

A) Thomas ensures that AV and AM software is used extensively within our infrastructure and is installed on all endpoints. Controls are in place to ensure that such software cannot be disabled/removed by end users to ensure the protection across the Estate.

Q) What protects corporate endpoints?

A) Microsoft Defender EDR with tamper protection and centrally managed policies.

Q) How do you manage patching

A) We benefit from being an Azure PaaS managed service, and patches are managed by Microsoft.

Q) How do you manage configuration changes?

A) Application images and configurations are maintained through CI/CD pipelines to avoid drift.

8. Secure Development & Change

Q) Do you follow secure development practices?

A) Yes. The SDLC integrates security by design and testing against the OWASP Top 10; all changes pass through peer review and automated CI/CD pipelines. No production data is used in test.

Q) Are environments segregated?

A) Yes—dev/test and production are segregated with separate access controls.

9. Business Continuity, Backup & Recovery

Q) How often are backups taken?

A) At least every 12 hours, with multiple restore points; integrity is validated by the service.

Q) What are your RPO and RTO for Assess & Connect?
A) RPO: 1 hour; RTO: target 4 hours under normal conditions.

Q) How do you test BCP/DR?
A) Plans are reviewed annually and exercised via tabletop and/or functional tests; uptime is monitored and P1 alerts trigger on-call response.

10. Vulnerability Management & Penetration Testing

Q) Do you perform vulnerability scanning and penetration testing?
A) Yes—regular scanning of internet-facing services and annual third-party pen tests on external scope; remediation is tracked to closure by severity. The latest Penetration Testing Summary Report can be found on the [Security & Compliance](#) section of our website.

11. Data Separation, Retention & Deletion

Q) How is client data separated?
A) Logical separation by client identifier at application and data layers. A) Assess and Connect operate as multi-tenant SaaS platforms with strict logical data separation enforced through RBAC, authentication boundaries, and tenant isolation.

Q) How long do you retain data?
A) Data retention is governed by contractual terms and documented retention schedules. Upon contract termination, personal data is deleted or anonymised in accordance with ISO 27001-aligned procedures.

Q) What happens to data when a contract ends?
A) Personal data is deleted or anonymised. Anonymised assessment artefacts (without identifiers) may be retained for analytics and product improvement.

12. Incident Response & Client Notification

Q) Do you have an incident response process?
A) Yes. Thomas maintains a documented Incident Response Plan with 24x7 coverage, defined escalation paths, forensic logging, and customer notification procedures.

Q) How quickly will you notify clients of an incident?
A) Clients are notified without undue delay once an incident affecting their data or service is confirmed, consistent with law and contractual terms.

Q) Please detail the number and length of any outages in the service within the last 24 months.
A) We have had no significant (unplanned) outages of the service within the last 24 months.

13. Artificial Intelligence (AI), Automation & Responsible Use

Q) Do Assess or Connect use Artificial Intelligence (AI)?

A) Yes. Certain features within Assess and Connect use AI-assisted capabilities to support insight generation, coaching, and interpretation of psychometric results. AI is used as a supporting tool and does not replace validated psychometric methodologies or human decision-making.

Q) What type of AI technology is used?

A) The platform uses a Large Language Model (LLM) deployed in a private, controlled environment. It operates using Retrieval-Augmented Generation (RAG) and Cache-Augmented Generation (CAG), meaning responses are generated only from approved, scientifically validated psychometric content, not from public or general training data.

Q) Is customer or candidate data used to train AI models?

A) No. Customer or candidate data is not used to train or fine-tune AI model weights. User input is processed dynamically during a session to provide contextually relevant responses and is not retained for model training purposes.

Q) Is AI processing performed in a closed environment?

A) Yes. All AI interactions occur within a secure, closed infrastructure. Prompts, responses, and system interactions are not exposed to public or uncontrolled AI services.

Q) Can AI features be disabled?

A) Yes. AI-assisted features can be disabled at tenant or user level and can also be temporarily disabled in response to a security or operational incident.

Q) How is AI accuracy validated?

A) Accuracy is ensured through a multi-layered approach:

- **Grounding responses in validated psychometric science**
- **Human expert review of outputs**
- **Automated accuracy metrics, including BERTScore and cosine similarity**
- **Ongoing testing prior to upgrades or parameter changes**

Q) How do you address bias and fairness in AI outputs?

A) Bias is mitigated through:

- **Restricting AI access to validated psychometric content only**
- **Guardrails to prevent speculative or non-evidence-based responses**
- **Continuous monitoring and testing against diverse datasets**