thomas
your business. your people. but better

Information & Data Security FAQs

Thomas' information security is outlined in **TT11_Information & Data Security,** 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, Holland, Malaysia, Hong Kong, South Africa and Australia.

CONTENTS

1. DATA PROTECTION

Q) Who is the formally appointed Data Protection Officer (DPO) at Thomas?
A) Head of Legal & Compliance ***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 use 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, in particular those relating to the General Data Protection Regulation ("the GDPR") and Data Protection Act 2018 ("the DPA")?
A) Yes

Q) Who in Thomas is responsible for the day-to-day security?
A) Chris Jackson, CTO **www.linkedin.com/in/chrisjj**

2. 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 work 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 take 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, these are incorporated into Thomas' employment contracts and Staff Handbook.

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).

3. 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 use 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. All Thomas offices utilise such measures as access control systems and alarms, with Thomas HQ and Developers Offices using CCTV also.

Q) Are all persons required to wear and display photographic ID at all times, whilst on company premises?
A) Yes, in the UK all employees and contractors are always required to wear SSID.

Q) In the event you use an external data centre (incl. Cloud) to store information please confirm your minimum data centre standard when appointing an external provider?
A) Tier 3

Q) Do you operate a clear-desk policy?
A) Yes, a clear desk policy is fully enforced across our UK offices.

4. INFORMATION SECURITY

Q) Describe how data is protected between any and all end user devices and the service.
A) Access to customer data is restricted to authorised users of the client Hub. All users are authenticated with username/password (details below), with logins not disclosing the existence of user accounts on failed logins. All data is encrypted to 256AES at rest and in transit, including backups.

Q) Where is the data physically stored and backed up?
A) MS Azure Public Cloud within EEA.

Q) Please outline which recognised security standards the data storage facility/data centre complies with.
A) MS Azure standards and certification.

Q) Is the organisation's Clear Screen Policy enforced through automatic user session suspension (e.g. automatic screensaver lock or remote access session termination) after a fixed period of inactivity?
A) Yes, automatic screen lock is set at 2 minutes for all UK based employees.

Q) Please describe how separation between service consumers is achieved.

A) All customer/candidate data within the Thomas environment is logically, rather than physically separated.

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 LUA (least-privileged user account) is embedded in the role profiles and functions are segregated to ensure security. Thomas also follow 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.

The Thomas solution is SaaS. As detailed above, Thomas ensure that all data is encrypted at rest and in transit using 256 AES encryption.

Q) Has the data storage facility or data centre been subject to any external audit? If yes, please describe the audit process and any recommendations/actions arising from the most recent audit.

A) Yes - MS Azure has been certified to numerous standards including ISO27001 - please see the following link for full details of MS Azure standards and certification.

Q) Please describe how data is disposed of when it reaches the end of its life.

A) At the end of the provision of service any candidate data is fully anonymised removing any and all PII, to only retain the assessment scores themselves which are used to further inform our product development and research. With the data having any and all PII removed, it ceases to be considered Personal Data as defined in the Regulation.

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

A) Thomas ensure 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 measures are in place to ensure effective protective monitoring of the service?

A) Thomas ensure we have monitoring systems in place to ensure we monitor system performance and thereby ensure system availability and a consistent user experience. We also use (as detailed elsewhere) IDS software to monitor our systems for suspicious activity.

Q) Please describe how the development of software or services in your organisation complies with any security standards, for example, ISO27034.

A) Thomas have a well-developed internal process for the development, test and release of software to the Live environment. As part of the development of software we ensure that security and Data Protection by Design and Default is as the heart of the process and also ensure that we develop and test against the Top 10 OWASP vulnerabilities.

Q) Please explain how your organisation ensures secure development of software / services.

A) Thomas ensure that all development is with regard to the OWASP Top 10 vulnerabilities and embeds Data Protection by Design and Default.

Q) Please describe how your organisation manages risk from third party suppliers and delivery partners.
A) Thomas have a robust supplier selection and ensure that all contracts with suppliers ensure compliance with relevant regulations including, but not limited to, the GDPR.

Q) How are users authenticated to the service (as defined) to prevent unauthorised access?
A) Access to the system is for authorised users with a secure username and password.

Q) How are user credentials protected? For example, Encryption, hashing etc.
A) All passwords are stored in encrypted form on the database. Passwords are never stored in plain text.

Q) How are user identities verified?
A) Users are identified via username and password - the system will never disclose the existence of a user from a failed login attempt.

Q) How are privileged administrative accounts secured? For example, Two or Multi Factor Authentication.
A) Thomas use two-factor-authentication for admin accounts and also whitelist access from trusted IP addresses.

Q) What is the password policy for the service provided by Thomas?
A) 8-25 characters. The password format for the Thomas system requires a combination of uppercase, lowercase and numbers. Passwords are obscured by default. All passwords are held in encrypted form and not plain text.

Q) Does the service employ certificate-based authentication? If so, please describe the methodology.
A) No, the solution is SaaS with appropriate measures in place to address (and exceed) the risks that the data processing poses to the data subjects rights and freedoms as defined in Art 32 (1) of the GDPR.

Q) Are all external interfaces (including Cloud based services) subject to penetration testing?
A) Yes, we have an annual penetration test by an external partner.

Q) Please describe your security incident management processes.
A) Thomas have a robust plan to deal with data security incidents. The details of our response plan are contained within an internal document and not for public disclosure.

Q) Please describe how you ensure duties are segregated between staff.
A) Thomas ensure that all access to systems is based on the principle of LUA (Least-privileged User Access) with access reviewed across AD on a regular basis and changes made to individuals' access when moving Team/Departments.

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 undertake regular reviews of Access Rights and any elevation rights is subject to an approval process.

Q) Please describe your starter, movers and leavers process in relation to IT permission/access levels.
A) As detailed elsewhere in this document we have regular reviews of access rights to ensure that access is appropriate. When colleagues move team or leave the company there is a well proven moving/off-boarding process to remove access to systems and data where required

5. CONTINGENCY & RESILIENCE

Q) Please state the name, job title and contact details for the person who has overall responsibility for Business Continuity, including IT Disaster Recovery.
A) Chris Jackson, CTO. Please note our BCP is an internal document containing sensitive information and for that reason cannot be shared.

Q) Please describe whether business recovery plans are documented and reviewed on a regular basis.
A) Yes, we review our BCP on a bi-annual basis.

Q) Contingency plans should be tested and reviewed on a regular basis, please confirm the date of the most recent exercise.
A) The BCP is reviewed bi-annually and tested quarterly. We also have the ability to very quickly re-deploy our entire system in a different data centre should we ever need to.

Q) Please confirm whether the same security processes, procedures and principles operate in any exercises and form part of any live invocation.
A) Yes, the procedures and principles would form part of the live invocation of the Plan.

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.