thomas™
your business. your people. but better

Thomas International Information & Data Security

Contents

Scope

This document explains Thomas' approach to information and data security, describing the technologies used to protect information and information systems. It answers questions that our clients regularly ask to satisfy their legal and regulatory requirements.

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.

Approval

Name	Job title	Date approved
Chris Jackson	Chief Technical Officer	March 2020
David Lowe	Head of Legal & Compliance	March 2020
Dave Anderson	Head of Business Services	March 2020

Version History

Version Number	Summary of changes	Issue date
V1 R0	Replaced: TTD04 _IT Security Doc V1 R1	March 2020

Message from the CTO

The confidentiality of our client's information is extremely important to us. Our systems and policies have been developed to protect this information as well as our own intellectual property.

We have implemented comprehensive Information Security to prevent unauthorised access to client information and to protect against evolving threats. We use a "secure by design" approach to our architecture to ensure that the security of data is considered at the design stage of our products and services. We employ a defence-in-depth strategy, which means that multiple layers of security protect our data assets in the cloud. The technology layers include firewalls, intrusion prevention systems, log monitoring, real time alerts, vulnerability scanners and anti-virus protection. Our commitment to cloud services allows us to stand on the shoulders of their security investments at the base layer, allowing Team Thomas to focus specifically on protecting your data.

The technical security solutions are complemented by industry-standard policies and best practices. Need-to-know and principle-of-least-privileges practices are followed throughout the company. Our Information Security is continually reviewed and validated by independent regulatory institutions and third-party security assessments organisations to ensure that we continue to meet or exceed security expectations.

We actively promote compliance with laws and regulations in various jurisdictions as well as our company policies. Our security policy and processes are designed to address the requirements of the European General Data Protection Regulation, our position as a data controller for the service indicates how seriously we take our responsibility to safeguard your information. We recognise client and business information security as a top priority and every member of Team Thomas is trained to understand their role and obligation to ensure this.

Thank you for your interest in Information Security Program at Thomas. If you have any questions, please do not hesitate to contact the information security team.

Chris Jackson
Chief Product & Technology Officer
infosec@thomas.co

1. Hosting Management

1.1 Location

Thomas use the Microsoft (MS) Azure West Europe Region, which is based in the Netherlands for the provision of our assessments to all customers and storing our back-ups. More detail can be found here.

However, Microsoft do not disclose the exact location of their datacentres – please see here. They state that *"Microsoft does not disclose the exact addresses of its data centres. We established this policy to help secure our data centre facilities."* This is an obvious approach and is in line with the well-known principal of Security Through Obscurity (STO); if the exact location of their datacentres is not widely known, this obviously helps further improve their inherent security.

Thomas, as many companies do, use sub-processors to provide their services and run their businesses. The sub-processors that we use to provide the assessment services directly to customers, include such suppliers as MS Azure.

1.2 Security & Access

MS Azure

Microsoft designs, builds, and operates datacentres in a way that strictly controls physical access to the areas where your data is stored. More details regarding the approach MS take can be found using this link.

Thomas UK Offices

While customer data is not hosted at Thomas offices, Thomas ensure that access to such offices is governed by, but not limited to, the following:

- Fob access and photo access cards are required by all personnel
- Visitors are required to sign in and out
- Physical access privileges are reviewed regularly

1.3 Compliance

Microsoft ensure their infrastructure is designed and managed to meet a broad set of International and industry specific compliance standards. These include, but not limited to the following:

- ISO 27001
- HIPAA
- FedRAMP
- SOC 1
- SOC 2

A more detailed overview can be found on the Microsoft site using this link.

2. Network Security

2.1 Perimeter Security

As detailed below Thomas ensure that security, resilience and availability are embedded into our systems and servers. The use of MS Azure as our CSP and the infrastructure and tools provided by Microsoft enable us to ensure a highly secure and resilient server builds.

Access Controls

Access to the MS Azure environment is for authorised users only, Thomas use a least privilege policy for access and permissions. All users who have access are enabled with MFA (multi-factor authorisation) and log in using a secure username and password.

Separation of environments

Thomas separates the production environment from any development and testing environments. The cloud environment is separate from Thomas' corporate offices and network.

Firewalls

Thomas use industry standard firewalls and/or security groups to prevent egress and ingress network traffic protocols except for those that are required by the business.

Hardening

Thomas infrastructure is automatically patched with the latest updates, PAAS (Platform as a Service) infrastructure is used meaning patching is managed directly by MS. Thomas ensure that there is no manual changes made to the infrastructure; everything goes through automation pipelines to ensure that there is no drift from the intended specification.

2.2 Server Monitoring

Vulnerability Detection & Management

Thomas runs an annual penetration test through by engaging with an independent third party. Thomas will monitor for any system vulnerabilities, with triggers and alerts in place to notify the relevant personnel. All alerts are logged and followed up by the incident response team, with any required fix following our development and release process.

Thomas have in place several systems, including IDS software which monitor the availability and performance of our systems, notifying key personnel within our IT Team in the event of reportable or suspicious incidents/activity. In addition, we utilise the tools and services within Azure and O365 to ensure appropriate monitoring and to ensure the security of personal data and also help to minimise the risk of data leakage out of the organisation (i.e. DLP).

Encryption

Thomas ensure that data is encrypted in transit and at rest using 256 AES encryption. Alongside this Transport Layer Security (TLS) 1.2 is leveraged for any customer data in transit.

The connection to the Thomas Hub is encrypted and authenticated using TLS 1.2, ECDHE_RSA with X25519, and AES_256_GCM.

3. System Security

3.1 Vendor Defaults & Secure Administration

Thomas International adheres to the following for all customer data that is stored, processed and/or transmitted on behalf of the customer:

- Maintains policies, procedures and standards to ensure all vendor supplied defaults are removed prior to installation of the system or system component
- Maintains policies, procedures and standards to ensure that vendor supplied relating to wireless networks are changed, including but not limited to default wireless encryption keys, passwords and SNMP community strings
- Maintains policies, procedures and standards to ensure that all administrative access uses strong cryptography (such as TLS for web-based administrative consoles, RDP with encryption enabled to access MS Windows systems)
- Maintains policies, procedures and standards to ensure that strong cryptography and security protocols (for example, TLS 2.0) are used when transmitting data over open, public networks, such as the Internet
- Utilise industry best practices (e.g. IEEE 802.11i) to implement strong encryption for authentication and transmission over the wireless network
- Prohibit the transmission of unencrypted / clear-text data via email
- Prohibit the transmission of unencrypted / clear-text data via other end-user messaging technologies, such as instant messaging and chat
- Maintain policies, procedures and standards to ensure that all systems are protected by anti-virus software
- Utilise anti-virus software that is capable of detecting, removing and protecting against all known types of malicious software (Trojans, worms, root kits, ad-ware, spyware, etc.)
- Perform checks at least daily to ensure that all anti-virus mechanisms are current, actively running, and generating audit logs

4. Access Management

4.1 Access & Authentication

Thomas use windows forms authentication and enforce password complexity where all passwords are stored using one-way encryption and must be between 8 - 25 characters in length with a combination of uppercase, lowercase and numbers.

Thomas also have a security process in place which will lock any Thomas hub account for 30 mins if the password has been incorrectly entered 10 times. This helps to prevent from unauthorised access to client accounts and data.

If you wish to reset your password, this can be done at any point via the Thomas hub. If you are not able to access the hub, there is a “forgotten password” button on the login page which will reset your account password and send this randomly generated password your email address.

The site uses a variety of methods to provide content to users. Among these Methods are;

- Secure Sockets Layer (SSL) – the site defaults to this protocol.
- FTP – for downloading reports to automated client servers.
- SMTP – for sending reports via email.
- Secure Shell (SSH) – for connecting to remote servers in order to send encrypted data (reports) to automated response clients.
- VPN – establishes a secure network tunnel between servers to allow access to data.

5. Backups

All backups are encrypted (256 AES) as detailed above. Backups of the system are taken at least every 12 hours with transactional data back -up data every 5-10 minutes. These backups are stored securely within MS Azure and retained for 7 days.

6. Organisational Management

6.1 Controlling Change

Thomas ensure that all development work is peer reviewed and developed against the Top 10 OWASP vulnerabilities.

6.2 Information Security Responsibilities and Awareness

Employment contracts and contracts with third parties state individual and organisational responsibilities for information security in accordance with the information security policy. This is outlined in the Covenant section of the employment contract.

Our data protection policy forms part of the Company handbook which is sent to all employees upon joining Thomas International and is also stored on our central employee database, which all employees can access.

Thomas ensure all personnel undertake cyber security training.
All Thomas personnel are required to sign a confidentiality agreement.
Access to Thomas systems/information is revoked immediately after contract.

7. Additional Sub-Processors

Thomas use a limited number of processors to provide our core assessment services to customers and are obligated to ensure as per art 28 (4) that such sub-processors are suitably qualified and there are compliant contracts in place.

Thomas International are confident that the contracts we have in place with the sub-processors used to provide the assessment services are compliant and in line with the obligations within the GDPR.

CONFIDENTIALITY & INTELLECTUAL PROPERTY

These materials have been prepared by Thomas for the exclusive and individual use of our client companies. These materials contain valuable confidential and proprietary information belonging to Thomas, and they may not be shared with any third party (including independent contractors and consultants) without the prior approval of Thomas. Thomas retains any and all intellectual property rights in these materials and requires retention of the copyright mark on all pages reproduced.

LEGAL CAVEAT

Thomas is not able to guarantee the accuracy of the information or analysis contained in these materials. Furthermore, Thomas is not engaged in rendering legal, accounting, or any other professional services. Thomas specifically disclaims liability for any damages, claims, or losses that may arise from a) any errors or omissions in these materials, whether caused by Thomas or its sources, or b) reliance upon any recommendation made by Thomas.