thomas
your business. your people. but better

Thomas International IT Security Document

Thomas International UK Ltd
1st Floor, 18 Oxford Road, Marlow, Bucks SL7 2NL
t +44 (0) 1628 475 366 e info@thomas.co.uk www.thomasinternational.net

SUMMARY

1. Data security

1.1. Hosting Management

1.1.1. Location, Facility and Constraints

Thomas International maintains and hosts its own physical servers for the business within Telehouse. The Telehouse London data centres have become the site for Europe's first carrier-neutral colocation facility, the home to the London Internet Exchange (LINX), as well as a backbone for the global internet network. Today, Telehouse operates four data centres in London – three at its Docklands campus in East London consisting of Telehouse North (opened 1990), Telehouse East (opened 1999) and Telehouse West (opened 2010) as well as Telehouse Metro (opened 1997) located near Silicon Roundabout in the City of London.

The site is the primary UK peering point for all UK tier one Internet Service Providers. The co-location cabinet connects directly to the UK internet backbone via two 100MB/s transit connections.

Thomas International Server Data is located across different floors in different buildings within the secure Telehouse environment to further mitigate risk from 'force majeure' type cyber-attacks and/or corruption.

For further or clarification information, please visit;

http://www.telehouse.net/london-data-centres

1.1.2. Host Security

As you would expect from a Tier 1 data centre, security on the Telehouse premises is of a very high standard, with Alarmed fences and PIR detection around the perimeter of the site, manned gated entrances with Security management systems in place which prevent any unauthorised access onto the site.

As well as this, the single point of entry to the main facilities is controlled by time limited access cards, movement activated CCTV around the perimeter, entrances and loading corridors. Doors to storage facilities are alarmed, and report back to a manned security suite immediately if unauthorised access is attempted or doors are forced/held open.

Finally, the Telehouse facilities are manned 24/7 by specially trained security staff, who ensure no unauthorised access to the site.

1.1.3. Host Access

Access to the facility is granted via a 3-level system of photographic log, access card and challenge/response passcode. Once access is granted all internal activity is monitored on the latest video surveillance. This is a Tier 1 graded facility.

1.1.4. Host Compliance/Certification

The Telehouse London Data Centres adhere to the following internationally recognised accreditations;

- ISO/IEC 27001:2013 (Information Security Management)
- ISO 22301:2012 (Business Continuity Management)
- PCI-DSS v3 (Payment Card Industry Data Security Standard)
- ISO 9001:2008 (Quality Management system)
- ISO 14001:2004 (Environmental Management)
- ISO 50001:2011 (Energy Management)
- BS OHSAS 18001:2007 (Occupational Health and Safety Management)
- RMADS (Public Sector Compliance)

1.2. Network Security

1.2.1. Perimeter Security (Firewall etc.)

The cluster is protected by a hardware firewall (Cisco Integrated Firewall and Intrusion Detection Software) which separates the web server from the 'outside world'. Thus, only data that meets security criteria passes through the firewall.

The server is also protected by software controls.

All passwords are stored in an encrypted format. Access to the database is locked down to respond to the web application controls only.

Our network hosting facility deploys VPN firewalls at your premises providing in depth defence for your environment, utilising Virtual Private Network (VPN) features to deliver increased peace of mind where required. We also have in place two CISCO integrated firewalls and intrusion detection software, as well as running a constant monitoring process using "PRTG" software to detect any outage / anomalies with our websites and servers.

The latest service and security packs are installed on the server machines and updated monthly using WSUS for deployment.

All unnecessary ports are closed; key default ports have been changed for critical functions.

All open ports are both password protected and configured to respond to only specific IP addresses.

All communications are carried out under SSL protocols, using a 128-bit key.

1.2.2. Server Monitoring

The site is monitored for excessive activity with automatic alarm procedures sent to both local hosting operators and our web development team in the UK.

Servers are monitored on a 24/7 basis. Server availability is monitored by "PRTG" software which physically tracks Server availability and "App Insights" which is a detailed tracking system for defects and usage trends. When a breach is detected; Thomas International will notify the client as soon as is practicable.

Error reporting is conducted through our regional and partner networks and/or raised directly with the webmaster. Once evaluated through our TSO (Team Services Online) ticketing system they are fixed and released through our continuous development cycle. The Client is then informed as soon as is practicable. The fix, if required, is released.

1.2.3. Hardware and Software

For the purpose of machine performance, anti-virus packages are not typically installed on server machines, as their extensive scan times can seriously degrade their responsiveness. All servers are however protected by;

- Latest Service Packs
- Latest Security Packs
- The standard Microsoft "Malicious Programme Removal" tool

1.3. System Security

1.3.1. Vendor Defaults and 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

1.3.2. Security Testing

Our security testing protocol involves running 'Gold Build' authenticated scans against representative workstation builds, including patch audits and custom Cyber Essentials Nessus scans. We also test each workstation for web and mail ingress filtering, by attempting to download and email various malicious file types respectively. All mobile devices in scope are tested for access control (pin codes) and patch management (up to date OS).

1.3.3. Other Third Parties

Our integration partners and distributors within the European Economic Area comply with GDPR 2016/679 in relation to Data Protection.

1.3.4. User Control

Thomas International will maintain the assessment and result data that is used by the user (Client) for evaluative purposes. Thomas International will endeavour to maintain the security of this data and information. We will never disclose this information to anyone except the user (Client) who subscribed to the service, unless we are required to do so by Law in accordance with Article 23 GDPR 2016/679.

Thomas International will not provide any personal information that specifically identifies the user (Client) to third parties to use for direct advertising or promotional purposes.

1.4. Processing, Storing and/or Data Transmission

1.4.1. System Configuration and Hardening

Thomas only open ports to servers running services from dedicated known locations. All outside access that is non-essential to the server performing a particular function are locked down through firewall rules. If extra functionality is required we only open the essential ports to enable the functionality and this is closely monitored to ensure only trusted communication is accepted by the receiving service.

Software we use;

- Beyond Compare Professional V3
- Browser stack – Cross browser testing tool
- Greensock Business Green
- Kentico
- RealObjects PDF Reactor
- Lastpass secure password store
- Particular software Service bus for .NET
- Tall Components Website PDF report generator NET 4.0
- Visual Studio Professional
- Visual Studio Test Professional
- Zopim Live Chat
- Microsoft SQL Server Enterprise
- 51 Degrees – device detection software
- Open ID – Oauth platform

1.4.2. System Patching

Thomas International perform monthly Windows updates (including hardware drivers) to keep our servers in line with Microsoft critical security and patches and manufacture recommended drivers. Every update is deployed and tested in a non-production environment prior to live deployment.

1.4.3. Software Development

Software is developed through our in-house development team. Utilising Microsoft technologies based on a .Net framework and TSO, we push a cycle through our DEV, QA and STAGING environments before a live deployment conducted in conjunction with our dedicated QA and Support departments.

When planned outages occur communications are sent out 2 weeks prior to the event then daily in the week leading up to the event. These planned outages usually occur outside of work hours over the weekend.

1.4.4. Coding guidelines

We encourage code-pairing where possible. All code is peer reviewed via a formal process which runs through a high-level checklist (QA and Regression testing comes after this stage). Code is deployed to all environments via an automated deployment process.

1.4.5. Resource Sharing

As an online client, your information is protected by your user account. When you become an online client, you will be given a username and a password that protects your information (see section 1.5.1). Your username identifies you as the individual to whom access to the information will be granted.

1.5. Access Management

1.5.1. Access and Authentication

We use windows forms authentication and we do 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.

We also have a security process in place which will locked 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.

1.5.2. Auditing, Access and Review

Makes available to the Service Administrator (Data Controller) all information necessary to demonstrate compliance with the obligations laid down in Article 28 (GDPR) and allow for and contribute to audits, including inspections, conducted by or on behalf of the Service Administrator (Data Controller).

As an Employer (Data Controller) and as a Service Provider (Data Processor) and, where applicable, our representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Provide a fully transparent, accessible and auditable "Subject Access Request" process in accordance with data protection legislation.

A fully auditable "Data Management" system that records all personal/sensitive data activity; processing, hosting, retention, transfer, deletion and enquiries in accordance with data protection legislation.

1.5.3. Unauthorised Devices and Changes

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.
- Webmaster and Development access is via IP LOCKDOWN.

Access to our servers are limited by 2 factor authentications, only allowing access through determined IP address and it is locked down with Windows authentication / password control.

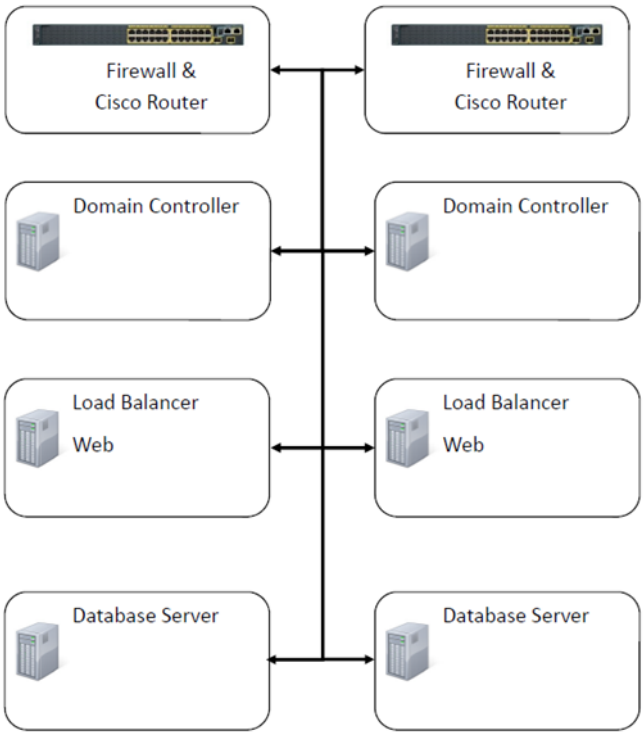
1.6. Physical and Logical Protection

1.6.1. Cryptographic Controls

All data in relation to the questionnaire is encrypted (Using AES 128 Encryption) and stored along with the main candidate data on our servers in Telehouse. Our Database servers use transparent data encryption which means that all data is stored in a permanently encrypted state (including in transit).

Everything related to the assessment is covered by SSL (encrypted with 128-bit encryption. The connection uses TLS 1.2 and is encrypted using AES_128_CBC, with SHA1 for message authentication and RSA as the key exchange mechanism.

For further information see;
https://msdn.microsoft.com/en-us/library/bb934049.aspx



1.6.2. Physical Security of Data

The Thomas infrastructure cluster is configured like the diagram shown running Microsoft SQL Server 2012 software using a Hyper Core / Multi Thread processors with Raid 10- array.

1.6.3. Physical Security (Visitor Procedures)

Please refer to sections 1.1.2 & 1.1.3 for information regarding physical access to Thomas servers.

1.6.4. Physical Security (Media – electronic/hardcopy)

Backups – cloud based and in Marlow office (locked server room), key fob access to office.

Movement of data – Salesforce for logs and policy in place to make sure only registered clients can request data.

1.7. Organisational Management

1.7.1. Controlling Change

TSO process and Sprint process – build / release process.

Windows updates process – test on stage then release and regression test live.

NB – major environment changes are notified to Client based on a 72hr timeframe (with the exception of third-party updates e.g. Windows).

1.7.2. 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.

Access to Thomas systems/information is revoked immediately after contract.

1.8. Back Up/Recovery Management

1.8.1. Back Up Management

Both Web and Database Servers use dual Serial ATA/SAS Drives to provide mirrored and/or arrays of hard disks. This technology is set up to provide disk mirroring as required. This provides constant protection against data loss.

Our databases are backed up incrementally on a 4-hour rolling time period. The backups are stored securely on site and sent to a secure server at our headquarters.

A network backup is performed to a remote server on another cabinet within the Telehouse premises daily. Further copies are taken from the database server to an external location in the UK weekly.

1.8.2. Recovery Management

Thomas have a secondary Disaster Recovery suite available in Witney, Oxon, allowing both staff and server re-location in the event of any issue with the primary hosting facility and/or Thomas offices.

1.8.3. Disaster Management

We have a load balanced environment that is software monitored sending out alerts to the technology team. If any major hardware failure occurs, we have hot swappable drives and redundant Servers onsite for immediate access.

Server Drives are located across different floors in different buildings within the secure Telehouse environment (see section 1.1.1. for further detail).

In the unlikely event of outages and or security incidents or any other downtime is communicated via our Global partner network and then disseminated to their clients in region.

1.9. Breach Management

Including (but not limited to);

• Loss or theft of data or equipment on which data is stored • Inappropriate access controls allowing unauthorised use • Equipment failure • Human error • Unforeseen circumstances such as a fire or flood • Hacking attack • 'Blagging' offences (spear phishing etc.) where information is obtained by deceiving the organisation who holds it.

Containment and Recovery;

- Set up Investigation Team – CTO, CO, IM, SDM
- Lockdown and secure all access to current systems/building (online and on premise)
- Notify third party service providers and agree further actions
- Restore data from secure back up system if required
- Prevent/Isolate further contamination
- Register lost equipment on immobilised property register
- Notify Police if required

Assessment of Ongoing Risk:

- Assess/identify lost data/equipment
- Assess sensitivity of data
- Re-evaluate encryption protocols
- Map data flow – type of data, stolen, damaged, total loss impact
- Assess potential exposure risks
- Whose/what data has been breached (including how many/scale of impact)
- Assess harm aspects (physical, financial, public etc.)
- Consider fraudulent aspects

Notification of Breach:

- Notify appropriate regulatory bodies (if/where applicable)
- Notify affected parties where applicable (employee, line manager, SLT, Stakeholders, Customer)
- Ascertain proportionate control measures for notification process
- Determine media response if appropriate
- Establish appropriate lines of communication (phone, email, social media etc.)
- Establish documented breach log including; times, order of events etc.
- Establish advisory levels for those affected
- Establish designated point of contact for ongoing help, support, queries etc.

Evaluation and Response:

- Assess personal data storage protocols
- Ensure data protection impact register is reviewed and updated if necessary
- Review current data disclosure protocols
- Review existing security measures
- Review training and awareness policies

2. Payment security

2.1. Payment Card Industry Data Security Standard Compliance

PCI DSS is the worldwide Payment Card Industry Data Security Standard that was set up to help businesses process card payments securely and reduce card fraud. This is achieved through enforcing tight controls surrounding the storage, transmission and processing of cardholder data that businesses handle. PCI DSS is intended to protect sensitive cardholder data.

(NB – this is an office based method for late payment recovery, this is not a process available through the Web).

The payment standard has 12 high level requirements which fall into the six categories below;

2.1.1. Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect data
- Do not use vendor-supplied defaults for system passwords and other security parameters

2.1.2. Protect Cardholder Data

- Protect stored data (use encryption)
- Encrypt transmission of cardholder data and sensitive information across public net

2.1.3. Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

2.1.4. Implement Strong Access Control Measures

- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

2.1.5. Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

2.1.6. Maintain an Information Security Policy

- Maintain a policy that addresses Information Security

The following are the 4 levels of PCI compliance:

Level 1: Merchants processing over 6 million card transactions per year

Level 2: Merchants processing 1 to 6 million transactions per year

Level 3: Merchants handling 20,000 to 1 million transactions per year

Level 4: Merchants handling fewer than 20,000 transactions per year*

*Thomas International UK Ltd are Level 4 PCI DSS compliant