a Williams Lea company

TSO (The Stationery Office)
18 Central Avenue
Norwich
United Kingdom
NR7 0HR
www.tso.co.uk

Dear Sir / Madam,

Please find the below company and service information needed for your completion of your supplier onboarding form.

If you require TSO to fill out your onboarding forms on your behalf, we can provide a quote.

Introduction

The online tools are owned by HSE and were developed by HSE's supplier Snap Surveys Limited, with TSO operating sales, marketing, and customer services functions as a support to HSE. Both Snap Surveys and TSO maintain ISO 27001 accreditation as part of our contractual requirements as suppliers to HSE as a UK government organisation. TSO is part of the Williams Lea group, as such TSO is bound by Williams Lea group policies.

This document sets out all the information you will require as part of your onboarding process including:

- Company details
- Risk and compliance
- Data security including GDPR
- Accessibility
- Availability
- Service maintenance and patching.

HSE's Stress Indicator Tool (SIT)

The Stress Indicator Tool is an online survey designed to gather data anonymously from employees, which can be used in the risk assessment element of HSE's Management Standards approach. Obtaining and understanding this information helps identify areas to improve to prevent and manage work-related stress. The reporting functionality is automated, so you don't have to spend time collating data or inputting the results manually. This helps avoid data entry errors, making the information collected more accurate and reliable. The report then summarises the views and experiences of employees and provides recommendations for future improvements. Read more

HSE's Safety Climate Tool (SCT)

The Safety Climate Tool has been carefully designed by scientists to assess the attitudes of individuals within an organisation towards health and safety issues. The Safety Climate Tool delivers an objective measure of your safety culture - the 'way things are done' in your organisation when it comes to health and safety. This is a significant starting point for any organisation to continually improve and raise standards. Using a simple, online anonymous questionnaire, the Safety Climate Tool explores your employees' attitudes and perceptions in key areas of health and safety. Once the survey has been completed, it generates a comprehensive report and provides guidance that will help improve the organisation's safety culture. Read more

Contents

About TSO

Company Details

Company name: The Stationery Office Ltd (TSO)

Registered address: 18 Central Avenue, Norwich, England, NR7 0HR

Registered website: www.tso.co.uk

Trading status: Limited Company

Date of registration in country of origin: 25th April 1995

Company registration number: 03049649

Head office DUNS number: 77-937-5633

Registered VAT number: GB 662774703

Details of immediate parent company:

Immediate parent company: Williams Lea Group Limited

Registered office address: 1- 5 Poland Street, Soho, London, England, W1F 8PR

Registration number: 01627560

Head office DUNS number: 227147899

Head office VAT number: GB662774703

Details of ultimate parent company:

Wertheimer UK Limited is a company registered in England and Wales. Wertheimer UK Limited was established as a special purpose vehicle to acquire the Williams Lea Tag business on 30th November 2017 and is solely controlled by funds managed by Advent International Corporation.

Registered office: 1- 5 Poland Street, Soho, London, England, W1F 8PR

Registration number: 10888457

Head office DUNS number: 223127563

Head office VAT number: GB 662774703

Risk and compliance

Modern Slavery Act 2015

Williams Lea are a relevant commercial organisation as defined by section 54 (“Transparency in supply chains etc.”) of the Modern Slavery Act 2015 (“the Act”). https://www.williamslea.com/modern-slavery

Insurance

Employer’s (Compulsory) Liability Insurance: £5m

Public Liability Insurance: £1m

Professional Indemnity Insurance: £5m

Assurance

- Quality Assurance ISO 9001:2008 – certificate number FS 569372
- Environmental Assurance ISO 14001:2004 – certificate number EMS 541713
- Information Security Assurance: ISO 27001:2005 – certificate number IS 650725
- Health and Safety Assurance OHSAS 18001:2007 – certificate number OHS 542150
- Business Continuity Management System ISO 22301:2012 – certificate number BCMS 637837
- Cyber Security: Cyber Essentials Plus – registration number QGCE 730
- Payment Card Industry Data Security Standards (PCI DSS) - LEVEL 1 SERVICE PROVIDER

Privacy policy

Privacy policy for TSO delivering the service on behalf of HSE.

https://books.hse.gov.uk/HSE-Books-Help-Pages/Privacy/

HSE’s privacy policy

https://www.hse.gov.uk/privacy.htm

Snap Surveys Limited privacy policy.

https://www.snapsurveys.com/survey-software/privacy-policy-uk/

For clarity, the only data the system holds, is the administrators work email address. You do not upload employee details into the system and all responses to the surveys are anonymous and no personal data is requested.

Assurance - Snap Surveys Limited

- ISO/IEC 27001:2013 Information technology, Security techniques, Information security management systems certification

Information security policy

Extract from Williams Lea Global Security Charter detailing our approach and policies.

Introduction

Data is the lifeblood of the modern digital economy, particularly in the sectors in which WL operates. We are entrusted with our Client's data and take this responsibility very seriously. The Board and Executive intend that WL is the most secure provider of media services and that our investment in security enables us to satisfy our risk appetite. It is fundamental to the success of our business that we:

- Protect our clients', employees', and partners' data diligently; and
- Ensure the confidentiality, availability and integrity of our data and systems.

Purpose

This Charter forms part of the WL Information Security Policy Framework and summarises WL's attitude, philosophy and the overall objective related to information security. The WL Security Charter is the foundation document for the overall WL Security and Information Security Management System, including its governance, programme, operations, and policy frameworks.

The Charter defines the Chief Information Security Officer's (CISO) responsibility and accountability for securing WL, and the supporting action required of other executives and departments. The Charter will be reviewed annually and reissued as required or when either the CEO or CISO transitions.

The Chief Information Security Officer is the owner of this document and is responsible for ensuring that this policy is reviewed and maintained.

This Charter supersedes and replaces all previous Charters on the same or similar subject matter.

Scope

To protect our clients' data and WL's assets, add value through a pragmatic, risk-based and business-aware approach to security, and, in doing so, inspire Client confidence and enhance our reputation in the market.

The objective is to reduce risk to an acceptable level according to WL's risk appetite by protecting the confidentiality, integrity, and availability of WL assets. It should be noted that it is neither possible nor practical to eradicate all risks and achieve 100% security.

Information security is managed as a principal risk, within WL's Enterprise Risk Management (ERM) system.

Communication

An awareness campaign will be established to ensure The Charter and supporting control documents are properly communicated and understood in order to educate and train the individuals, groups, and organisations covered by the scope of this Charter.

Principles

The following principles have been established by the CEO, and applied to the WL security framework:

- WL will aspire to the highest standards of quality and integrity, and these standards extend to security capability and processes.
- WL has a responsibility to protect our clients' and employees' data and, consequently, security is not something to compromise on.
- WL will act with integrity in the event of any incident that discloses customer data, working promptly and openly to communicate and to resolve.
- WL fully understands that the impact of a data breach would be significant and highly damaging, financially and reputationally.
- Everyone within the business (from the top to the bottom) is responsible for the security of WL,

employee and client data and for maintaining a strong security culture.

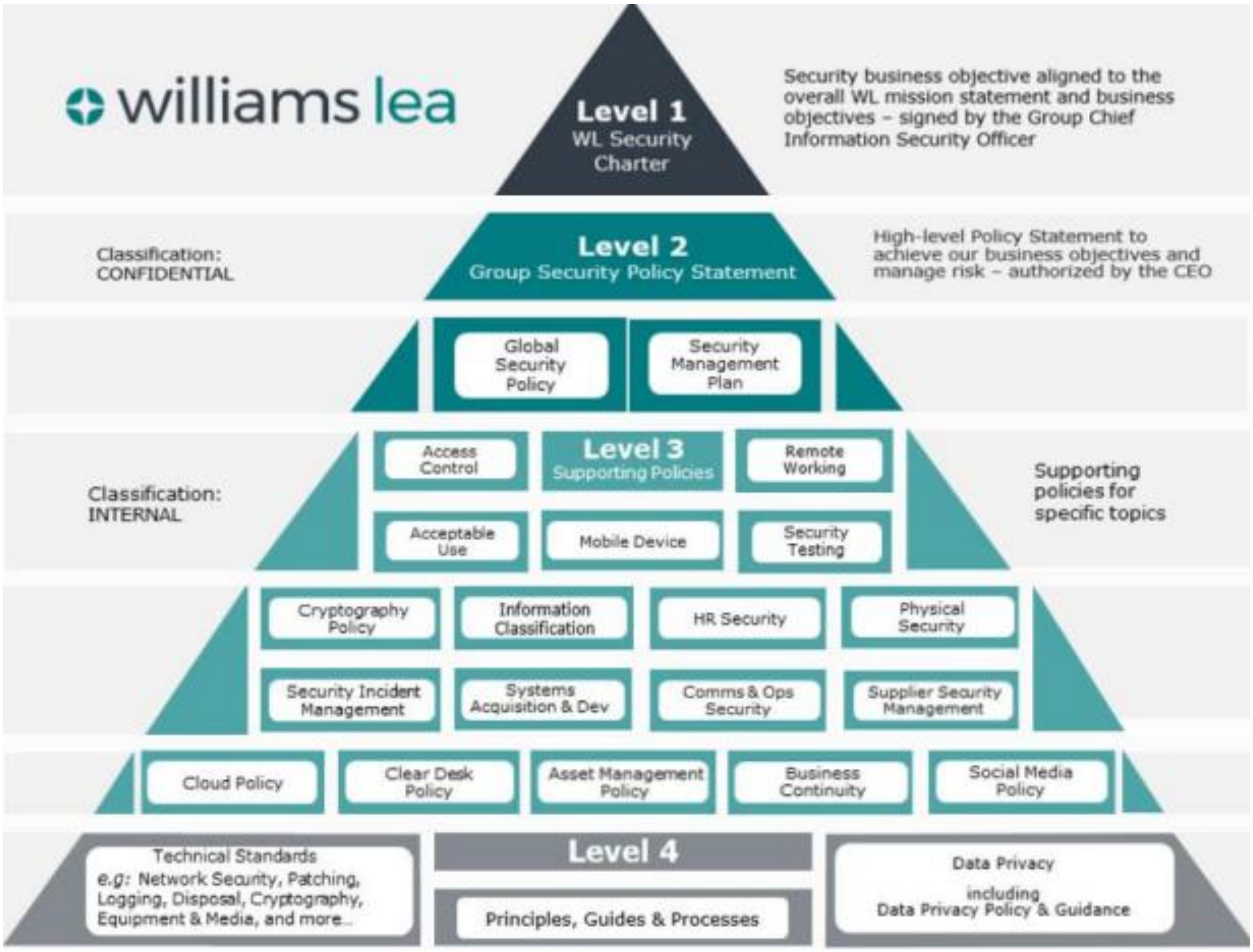
- Strong security should be viewed as a competitive advantage.
- The Board and executive will actively oversee the security program to ensure that security risk/vulnerability is mitigated as quickly as possible and will allocate the time necessary to lead, monitor and assure this process.
- Security standards and policies will be mandatory wherever possible or appropriate, and that any significant conflict between business and security priorities should be analysed and decisions escalated if appropriate compromises cannot be achieved.
- Security requirements need to be proportional, affordable, and appropriate to our sector and aligned to delivery of our risk appetite.

Policy framework

This security charter is the Level 1, authoritative statement of security strategy and direction it is supported by a suite of policies and Technical Standards and Patterns. The WL Security policy hierarchy is:

Level 2: Global Security Policy, Security Management Plan, and Group Security Policy Statement

Level 3: Acceptable Use, Access Control, Asset Management, Business Continuity, Clear Desk, Cloud, Communications and Operational Security, Cryptography, HR Security, Information Classification and Data Sensitivity Labelling, Mobile Device, Physical Security, Remote Working, Security Incident Management, Security Testing, Supplier Security Management, and Systems Acquisition & Development



Security business objective aligned to the overall WL mission statement and business objectives – signed by the Group Chief Information Security Officer

High-level Policy Statement to achieve our business objectives and manage risk – authorized by the CEO

Please accept this as evidence the relevant policies, procedures and protections are in place.

Data Security

GDPR

The service does not store or access any personally identifiable data, as such GDPR is out of scope.

- TSO/Williams Lea is registered with the information commissioner Z9116702
- Nominated Data Protection Officer (DPO) global.privacy@williamslea.com

The data we hold

No personal data: the only data the system holds is the administrators work email address, you do not upload employee details into the system and all responses to the surveys are anonymous and does not include any personal data.

TSO processes your account data, payment, company details in out inhouse systems hosted in AWS datacentres in the UK. For confirmation AWS holds and maintains ISO 27001 accreditation.

Security accreditation and certification

- TSO, Snap Surveys, and the data centers all hold and maintain ISO27001 accreditation.
- TSO holds Cyber Essentials certification

Hosting

Snap Surveys' UK based data centres are hosted at Microsoft Azure and ANS Group (previously UKFast), all of which are ISO 27001 certified. Snap carefully selected their hosting providers as they offer the same high standards of information security, so you can be sure your data is safe.

Location UK

The service is hosted in the UK on a secure site and with no data from the services being processed outside of the UK. Please note that your organisations administrator of the service can access the system outside of the UK to download survey reports.

Penetration test

When there are service changes and on an ongoing basis, automated vulnerability tests are completed, and risks managed in accord with good industry practice. Due to the secure nature of the data included in the penetration tests these cannot be shared with external organisations.

Snap regularly tests its software for vulnerabilities, these tests are performed by CREST accredited suppliers. In addition, ongoing vulnerability scanning is completed by Invicti https://www.invicti.com/

Multi factor authentication (MFA)

MFA is in place for the administrator, any changes needed outside of this such as an employee leaving, will require the written permission for at least two directors of your organisation to ensure data (organisational scores) are protected.

Data encryption

Data in transit: the online web based system has a secure SSL connection to encrypt data. Up to TLS 1.2

Data at rest: Advanced Encryption System (AES)

Endpoint Protection: Firewall & Anti-virus systems

Data retention

There is no personal data requested by the system. The data is held for a maximum of 7 years and can be deleted by your organisation administrator at any time.

Accessibility

Snap web questionnaires can conform to version 2.1 of the Web Content Accessibility Guidelines (WCAG) meeting level AA compliance, with the addition of being compliant to many of the AAA level checkpoints.

The Snap Surveys Accessibility Statement which gives details on how to achieve compliance for web questionnaires published by Snap. https://www.snapsurveys.com/snap-surveys-accessibility-statement/

Snap Surveys is committed to providing web products that are accessible to the widest possible audience, regardless of technology or ability. We are actively working to increase the accessibility and usability of our web products and in doing so adhere to many of the available standards and guidelines.

Availability

The service is hosted in a high-security UK-based ISO-certified, tier 3 data centre, built on enterprise-grade infrastructure for speed, resilience, and super-fast connectivity.

Capacity & uptime monitoring systems are in place to confirm sufficient resource, speed of service and availability.

Multiple layers of redundancy give us a service target of 100% uptime, excluding planned maintenance.

Service maintenance and patching policy

As a subscriber to the online tools, you will be informed of scheduled maintenance in advance. We will seek to reduce any impact by completing any maintenance and service updates during holiday periods where it is strongly recommended that active surveys are not completed.

Security updates for all systems are installed, and systems rebooted (if required) within the following timeframes. All security patches are applied within 30 days of release. Critical vulnerabilities are patched within 14 days of patch release. These timescales may be adjusted if required by the IT Security team.

Performance measures

Performance measures are not applicable under the terms of the license with HSE.

SLA’s

Not applicable, as detailed in previous sections, there are maintenance plans, capacity plans and business continuity plans are in place. No further SLA’s will be provided.

Past performance

Uptime of the platform in 2021 was 99.95% and in 2022 (up to the end of September) it has been 99.98%

Maintenance windows are scheduled for Sunday mornings between 07:00 & 09:30. Please note that not all windows are used, and downtime is kept to an absolute minimum during the windows.

P1 Incidents

Not applicable

We confirm the information provided in this document was correct at the time of signature and will be reviewed and updated as required.

Signed on behalf of Williams lea / TSO

Name Ian Fik Account Director

Date 27/03/2023

Signed on behalf of HSE

Name Charles Oakley

Date 3rd April 2023