SYSTRA

SYSTRA LIMITED - UK & IRELAND

DATA SECURITY POLICY

November 2019

OUR COMMITMENT

Data are a vital part of SYSTRA Limited's business. Data can be information that we have obtained through surveys or other methods of primary data collection; it can be provided to us by our clients in connection with the work that we do for them or it can be internal to SYSTRA Limited (such as information about our staff).

Our staff, clients and respondents expect us to treat such data with the utmost care and caution and in compliance with the law.

In order to protect data that we hold from unauthorised loss, destruction, or disclosure, it is imperative that we have a Data Security policy governing how our staff capture, store, process, transmit, and destroy data.

Our Data Security policy ensures that we have appropriate technical and organisational measures in place to safeguard personal data. It also covers any other data storage device or medium such as paper reports.

The only information that we have that is classified as personal data is held and used only for research purposes and collection of such data is purely for confidential survey research.

The only exception to this is data concerning our own staff, held and used by the Human Resources Department. All identifiable data is held using appropriate security measures.

Personal information provided to us by clients for processing is also covered by our policy. In such cases we and the client agree and document a security, retention, and destruction process in line with the General Data Protection Regulations (GDPR). This must be agreed with the client before any data are exchanged.

SYSTRA Limited is registered under the Data Protection Act 1998 for all purposes for which we use personal data. The registration number is Z7084167. A copy of the certificate is held in our document management system (Sharepoint) and is available for inspection.

In addition, SYSTRA Limited is certified against the UK Government Cyber Essentials scheme.

Staff are required to familiarise themselves with the handling of data and ensure that the guidelines laid out in this policy are followed. All market research work is also done in accordance with the Code of Conduct of the Market Research Society (and its associated guidelines), the Ethical Guidelines of the Social Research Association, and the GDPR regulations.

Responsibility for the implementation of our data security policy is held by the CEO and is reviewed and amended by the Senior Management Team once a year. The policy is posted in our corporate Sharepoint site, which is available to all staff.

INFORMATION ASSET OWNERS

Personal data obtained and used in the course of our operations are always attributable to a project.

The Project Manager is the Information Asset Owner. The Project Manager reports to the Project Director who monitors the implementation of the Data Security Policy for the project. For internal data the Information Asset Owner is the Head of Department.

INFORMATION PROTECTION IMPLEMENTATION MEASURES

The Project Manager and Project Director agree on and keep a record of those members of the project team allowed access to protected data.

Each project has to have a Project Risk Assessment (PRA) form, which is completed before the project begins. This is a requirement of our Integrated Management System (IMS). Appropriate procedures are set out in the IMS manual and all Project Managers have been trained in these procedures. Data and information risk is covered in the PRA. For projects that last more than three months the Project Manager and Project Director review the confidentiality, integrity, and availability of information at intervals of no more than three months.

STAFF AWARENESS

All staff are aware of the need to protect all data collected by us or supplied to us by our clients and the requirement to treat any such data as confidential and sensitive. This is stated in each person's contract of employment. Additionally, all staff are fully instructed on this requirement.

We enforce this through completion of an online GDPR training course for all staff at all grades. We monitor completion rates for this course on a regular basis.

Staff are instructed in safe data handling methods and we run mandatory training courses in IT Security for all staff.

COMPLIANCE AND EFFECTIVENESS MONITORING

Project staff's compliance with the requirements is supervised by the Project Manager and Project Director. Compliance is an integral part of our IMS. A proportion of all projects are subject to audit on a rolling programme that takes place several times a year.

SUBCONTRACTORS

Subcontractors are chosen from the Approved Business Partners List. A requirement for being placed on, and remaining on, that list is that they comply with our company policies (one of which is this Data Security policy), or have equivalent and acceptable policies of their own.

STORAGE AND DISPOSAL OF PROTECTED DATA HELD ON PAPER

Protected data (including questionnaires) held on paper are either kept on premises that are secured 24 hours a day or (in offices that are not so secured) are locked away when not being used.

Disposal of protected data held on paper is normally destroyed by dedicated shredding companies. We receive certificates of destruction for all such activity.

STORAGE AND DISPOSAL OF PROTECTED DATA HELD ON ELECTRONIC SYSTEMS

Anti-Virus/ Anti-Malware Protection

All SYSTRA Limited PCs, laptops and servers are protected by Anti-virus software. This software cannot be removed or disabled by users. Periodic virus scans are performed automatically and must be allowed to complete.

All PCs, laptops, and servers are updated in real time (or in the case of laptops, when they log on) with the latest version of anti-virus/anti-malware software.

In addition to this, all incoming and outgoing email is scanned for viruses by filters and scanning engines by a specialist provider of managed IT security services. Suspect email and/or attachments are not delivered but are held in a queue; the sender and recipient are both informed.

Security Against Loss or Theft

All laptop computers are password protected by Active Directory (AD) passwords and (where possible) encrypted using BitLocker. Our ICT department sets this on all laptops through use of a standard SYSTRA image for computers. Users' AD passwords must not be written down or shared with anyone (including SYTSRA employees) Staff must inform the ICT department immediately if they have had a laptop stolen or lost. ICT will then immediately ensure that all user access from the laptop to SYSTRA Limited's systems is revoked. This can be re-instated should the device be found.

The user will be given new security settings. Laptops must not be left unattended when off-site in public places and should be locked away in a secure area when unattended off-site. On no account must they be left unattended on trains, in cars or in hotel rooms unless in a safe.

Unattended laptops and PCs should be powered off where possible to conserve energy. In the event that a laptop is left powered on and unattended, the workstation will automatically lock, requiring the user to re-enter their AD credentials.

Transferring Electronic Files or Documents

Staff are aware that wherever possible transfer of sensitive data between sites should be minimised.

Where transfer of data outside the SYSTRA network is required, data should be transferred using SYSTRA's online tools (SendTo and/or SharePoint). For very large data transfers, staff must liaise with the ICT team.

Personal data must not be taken out of the office on laptops or removable electronic media unless it has been encrypted using SYSTRA-approved encryption software.

Personal details that are stored on removable media and sent to other agencies or clients must be sent via an approved courier or delivered by hand. The files on the removable media must be encrypted.

Transfer of data outside the immediate SYSTRA Limited project team requires the prior approval of the Project Manager.

DATA SECURITY POLICY

Deletion of Files and Disposal of Protected Data

Data files or documents that contain sensitive data are removed using File Shredding software to remove files securely from hard drives and removable media.

When they are no longer required, electronic media used for storing protected data are destroyed by shredding of the hard drives by a specialist company. A signed record of the destruction is kept.

Access Control

Access control is maintained on the servers, PCs and laptops, via individual user IDs and passwords.

Passwords are force changed every six months and have minimum complexity rules.

Access levels are given to the user as appropriate to their job and grade. Files held in Sharepoint or the financial system (Agresso) are controlled by an appropriate level of user roles and user rights. All servers are backed-up overnight using commercial cloud storage (Amazon S3/Glacier) The computer rooms in each office have restricted access (via locked door or keypad). The buildings are alarmed and the floors housing the computer suite are locked out of hours.

BUSINESS CONTINUITY

We have a policy that governs how and when data residing on company servers will be backed up and stored for the purpose of providing restoration capability. In addition, it addresses methods for requesting that backed up data be restored to individual systems.

Daily backups of all servers are performed on all sites. All staff are provided with access to Microsoft OneDrive for backup of personal files/work-in-progress.

SYSTRA Limited has several offices in the UK and Ireland. As the company has multiple office locations, it would continue to operate from surviving locations should one or more be lost as a result of an incident.

SOFTWARE POLICY

SYSTRA Limited has a strict software and password access policy which has been signed by all existing staff; new staff sign it on commencing employment.

SYSTRA Limited is a member of FAST (Federation Against Software Theft) and has a commitment to ensure the legal use of software and data, and correct use of email and Internet facilities by staff.

FIREWALLS

Our systems in the UK and Ireland are protected by industrial-grade firewalls, managed in secure data centres.

This policy is communicated to all employees and organisations working for SYSTRA Limited or on our behalf.

This policy is reviewed annually by the SYSTRA Limited Management Board and is available to interested parties upon request.

NICK SALT
CEO, SYSTRA Limited
22 November 2019