1. Security and Confidentiality Policy

1.1 Confidentiality

The success of IDOX is due, in part, to maintaining strict confidentiality with client information and between client projects.

Every employee has a responsibility to the company, its suppliers and customers to treat all information received as confidential.

It is IDOX's policy to treat any client or supplier's information with sensitivity and not disclose this internally or externally unless the information already exists within the public domain.

It is the role of the project manager (PM) to ensure all staff involved with a project are briefed on any special security or confidentiality agreements. The PM should also remind staff at the beginning of each project of this policy and confirm they have read and understood its contents.

It is common practice to make use of Non-Disclosure Agreements, and these can take the form of client's agreements or the IDOX standard agreement.

1.2 Data Protection

1.2.1 Introduction

The Group has to collect and use certain types of information about clients, staff and general members of the public in order to conduct business. The information collected is about people with whom the Group has had contact in the past and is likely to in the future. This includes current customers and suppliers, employees, prospective clients and others with whom the company interacts in the normal conduct of business.

In addition, in the provision of support to our customers we sometimes have access to their customers' personal data.

The Group also collects data to ensure compliance with other current and past relevant legislation.

This data ('Personal Data') will be collected, stored and used in full compliance with the Data Protection Act 1998 {The Act).

The Group recognises a moral duty to ensure that all such data is handled properly and confidentially at all times whether on paper or in an electronic format.

1.2.2 Principles

The Group will manage Personal Data in full compliance of the Act throughout the following:

- Obtaining of Personal Data;
- Storage and security of Personal Data;
- Use of Personal Data, and
- Disposal/destruction of Personal Data not required for the conduct of business.

The Group will allow data subjects with appropriate access to details regarding personal information relating to them.

The Group fully endorses and will adhere to the data protection principles set out in The Act, in particular, to the principles relating to personal information.

1. The Group shall process all Personal Data fairly and lawfully
2. The Personal Data will only be obtained for one or more specified and lawful purposes and shall not be further processed for any other purpose which is incompatible with the normal legal conduct of The Group's business.
3. The Personal Data will be adequate, relevant and not excessive for the purpose(s) for which it is to be processed.
4. The Personal Data shall be accurate and kept up to date
5. The Personal Data shall not be kept longer than is absolutely necessary or required by other current legislation.
6. The Group acknowledges the rights of individuals to whom the Personal Data relates, and ensures that these rights can be exercised in accordance with the Act.
7. The Group has put in place technical and organizational measures to ensure against unlawful or unauthorized processing of Personal Data and against accidental loss or destruction or damage to all data
8. The personal Data held by the Group will not be transferred to a country outside the European Economic Area.

1.2.3 How this will be achieved

The Company will follow and maintain strict safeguards and controls by:

- Nominating a 'Data Protection Officer' of sufficient seniority who is responsible for gathering and disseminating information and issues relating to information security, The Act and other related legislation. The nominated officer is Richard Kellett-Clarke, Director responsible for all operational matters
- All Senior Managers are responsible for communications and issues relating to information security, The Act, and other relevant legislation within their area of responsibility.
- The Group will ensure that all activities that relate to processing of personal data have safeguards and controls in place to ensure full compliance with the Act.
- The Group ensures that all employees understand their individual responsibility relating to the requirements of The Act. Employees are provided with appropriate training, instruction and supervision so that duties are carried out effectively and consistently. Staff will only be given access to personal data that is appropriate for the effectively completion of their duties and tasks.
- The Group ensures that third parties (mainly suppliers) endorse the principles set out in the Act. In addition, third parties will only be provided with appropriate and minimal information for the duties/tasks to be undertaken.
- The Group will handle all requests for access to personal data courteously, promptly and appropriately. The Group will ensure that the data subject or an authorized representative has a legitimate right of access under the Act, the request is valid and the information provided is complete, clear and unambiguous. The Group will log all requests, the steps taken to validate the request and the information provided and/or withheld with reasons.

This Data Protection Policy will be reviewed regularly, in accordance with the Group's Information Security Management Policy, to ensure that the safeguards and controls in place are adequate, relevant and effective.

1.3 Security

Introduction

The Idox Group Information Security Policy applies to all business functions within the scope of the Information Security Management System and covers the information, information systems, networks, physical environment and people supporting these business functions. This document states the Information Security objectives and summarises the main points of the Information Security Policy.

Objective

The objective of Information Security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. In particular, information assets must be protected in order to ensure:

1. Confidentiality i.e. protection against unauthorised disclosure
2. Integrity i.e. protection against unauthorised or accidental modification
3. Availability as and when required in pursuance of the Organisation's business objectives.

Responsibilities

1. The Board of Directors have approved the Information Security Policy.
2. Overall responsibility for Information Security rests with the Quality Manager.
3. Day-to-day responsibility for procedural matters, legal compliance including data protection, maintenance and updating of documentation, promotion of security awareness, liaison with external organisations, incident investigation, management reporting etc. rests with the Information Security Management System Manager.
4. Day-to-day responsibility for technical matters, including technical documentation, systems monitoring, technical incident investigation and liaison with technical contacts at external organisations, rests with the Head of Internal IT.
5. All employees or agents acting on the Organisation's behalf have a duty to safeguard assets, including locations, hardware, software, systems or information, in their care and to report any suspected breach in security without delay, direct to the Head of Internal IT or the Information System Management Manager. Employees attending sites that are not occupied by the Organisation must ensure the security of the Organisation's data and access their systems by taking particular care of laptops, blackberries and/or similar computers and any information on paper or other media that they have in their possession.
6. The Information System Management Manager is responsible for drafting, maintaining and implementing this Security Policy and similarly related documents as detailed in Appendix II.
7. As with other considerations including Quality and Health & Safety, Information Security aspects are taken into account in all daily activities, processes, plans, projects, contracts and partnerships entered into by the Organisation.
8. The Organisation's employees are advised and trained on general and specific aspects of Information Security, according to the requirements of their function within the Organisation. The Contract of Employment includes a condition covering confidentiality regarding the Organisation's business.
9. Adherence to Information Security procedures as set out in the Organisation's various policies and guideline documents is the contractual duty of all employees and a clause to this effect is set out in the Organisation's contracts of employment.
10. Copies of the Information Security Management Manual, including are made available to all of the Organisation's employees.
11. Breach of the Information Security policies and procedures by the Organisation's employees may result in disciplinary action, including dismissal.
12. In view of the Organisation's position as a trusted provider for the development and sale of products for document, content and information management, providing innovative e-government and e-business solutions that allow the delivery of information to the citizen and clients across the Internet, extranet or intranet, particular care is taken in all procedures and by all employees to safeguard the Information Security of its service users and/or clients.
13. Agreements of Mutual Non-disclosure/Confidentiality are entered into as appropriate with third party Companies.
14. All statutory and regulatory requirements are met and regularly monitored for changes.

15. A Business Continuity Plan is in place. This is maintained, tested and subjected to regular review by the Information System Management Manager.
16. Further policies and procedures such as those for access, acceptable use of e-mail and the internet, virus protection, backups, passwords, systems monitoring etc. are in place, maintained and are regularly reviewed by the Information System Management Manager and the Head of Internal IT or an appointed representative, as appropriate.
17. This Information Security Policy is regularly reviewed and may be amended in order to ensure its continuing viability, applicability and legal compliance, and with a view to achieving continual improvement in the Information Security Systems.

Signed

Andrew Riley, Chief Executive Officer

9th January 2017

QMS INTERNATIONAL

A CITATION COMPANY

ISO 27001 REGISTERED

This document certifies that the information security management systems of

IDOX SOFTWARE LIMITED
2nd Floor, Waterside 1310, Arlington Business Park, Theale RG7 4SA

have been assessed and approved by QMS International Ltd to the following information security management systems, standards and guidelines:-

ISO 27001 : 2005

The approved information security management systems apply to the following:-
THE DEVELOPMENT AND SALE OF PRODUCTS FOR DOCUMENT, CONTENT AND INFORMATION MANAGEMENT, PROVIDING INNOVATIVE E-GOVERNMENT AND E-BUSINESS SOLUTIONS THAT ALLOW THE DELIVERY OF INFORMATION TO THE CITIZEN AND CUSTOMERS ACROSS THE INTERNET, EXTRANET OR INTRANET

Original Approval: 27 May 2011

Current Certificate: 10 June 2015

Certificate Expiry: 26 May 2021

Certificate Number: 14127474

On behalf of QMS International Ltd

This Certificate remains valid while the holder maintains their management system in accordance with the published standard. To check the validity and status of this certificate please email certificates@qmsuk.com

This Certificate is the property of QMS International Ltd and must be returned in the event of cancellation