

Legal

IGOV0022 - Idox International Business Conduct Policy

Document Type: Policy

Document Description: Covering Business Conduct including Anti-bribery & corruption, Whistleblowing, Anti-slavery & human trafficking, Occupational H & S, Equality & diversity, Security & confidentiality, Environmental, Inside information & share dealing

Searchable Tags: CoC GDPR DPA ISMS

Last Reviewed: 1 September 2024

Next Review Due: 20 June 2025

Version: 5

Classification: **Public**

Document control

Version	Changes	Author	Date
0.1	Imported into SharePoint document management system	NIBE	10/08/2021
0.2	Full Content review – info sec	NIBE	10/08/2021
1.0	Full content review – legal	THLA	31/08/2021
2.0	Link corrections – Updated DPA, Info Sec, and Environmental Policies.	NIBE, ELHU	08/12/2022
3.0	Reviewed InfoSec and DPA and Environmental policies, updated all ISO certification marks logos to align with new assessor branding.	NIBE, ELHU, RABE	20/08/2023
4.0	Update InfoSec, OHS and Environmental policies. E&D Policy update, general legal review.	NIBE, ELHU, TAGI	23/07/2024
5.0	Section on Fraud Prevention added	TAGI	02/09/2024

Copyright

Ideas, solutions, suggestions, hints and procedures from this document are the intellectual property of Idox plc and thus protected by copyright. They may not be reproduced, transmitted to third parties or used in any form for commercial purposes without the express permission of Idox Group.

Contents

1 Our Commitment and Policies	5
1.1 About Idox	5
1.2 Responsibilities	5
2 Ethical Business Conduct	6
2.1 Anti-Corruption	6
2.2 Bribery Act 2010 ("BA Act")	6
2.3 Constraints and Conflicts of Interest	6
3 Whistleblowing	7
3.1 About this Policy	7
3.2 What is whistleblowing?	7
3.3 How a concern is raised	7
3.4 Confidentiality	7
3.5 External Disclosures	7
3.6 Protection and Support for Whistle-blowers	7
3.7 Contacts	8
4 Anti-slavery and Human Trafficking	9
5 Fraud Prevention	10
6 Occupational Health and Safety	11
7 Equality and Diversity	12
7.1 Code of Practice	12
7.2 Management Responsibility	13
8 Security and Confidentiality	14
8.1 Confidentiality Policy	14
8.2 Data Protection Policy	15
8.2.1 Policy Statement	15
8.2.2 Scope	15
8.2.3 Data protection principles	15
8.2.4 General provisions	16
8.2.5 Lawful, fair and transparent processing	16
8.2.6 Lawful purposes	16
8.2.7 Data minimisation	17
8.2.8 Accuracy	17
8.2.9 Archiving / removal	17

8.2.10 Security.....	17
8.2.11 Sub-processing.....	17
8.2.12 Data Sharing	18
8.2.13 Subject Access Requests (SARs).....	18
8.2.14 Responsibility for the processing of personal data	18
8.2.15 Personal Data Breaches	19
8.2.16 Monitoring and review	19
8.2.17 Enforcement.....	19
8.3 Information Security Policy.....	20
8.3.1 Purpose.....	20
8.3.2 Scope.....	20
8.3.3 Objective.....	20
8.3.4 Responsibilities.....	20
8.3.5 Principles	21
8.3.6 Information Security	21
9 Environmental Safety	23
9.1 Environmental Policy Objectives	23
9.2 Environmental Management System Accreditation.....	24
10 Inside Information and Share Dealing	25
11 Contact us	27

1 Our Commitment and Policies

Idox plc and its [subsidiaries](#) (hereinafter referred to as 'Idox' or the 'Organisation') has introduced its International Business Conduct Policy to guide our accountable and responsible business practices. The regulatory landscape is changing and Idox is committed at being at the forefront of corporate compliance.

1.1 About Idox

Idox is a leading supplier of digital software and services to a diverse customer base in both the UK and International markets. Spanning both the public and private sectors, Idox works across a range of industries and sectors – from central and local government to transport, health and social care and commercial organisations, to deliver smart technology that enhances services and improves productivity.

1.2 Responsibilities

Every employee of Idox has the responsibility to ask questions, seek guidance, report suspected violations, and express concerns about this policy and its related procedures. This International Business Conduct Policy is underpinned by detailed Idox policies and procedures which assists employees in resolving questions and in reporting suspected violations. Managers are responsible for supporting implementation and monitoring compliance.

2 Ethical Business Conduct

The Group conducts its business fairly, impartially, in an ethical and proper manner, and in full compliance with all laws and regulations. In conducting its business, integrity is the foundation of all company relationships, including those with customers, suppliers, communities and employees.

The highest standards of ethical business conduct are required of Idox employees in line with their company responsibilities. Employees will not engage in conduct or activity that may raise questions to the Organisation's honesty, impartiality, or reputation or otherwise cause embarrassment to the Organisation. Conduct that is prohibited under this policy must not be carried out by anyone externally on behalf of the Organisation.

2.1 Anti-Corruption

Each member of Idox conducts its business in compliance with applicable anti-corruption laws and has instituted and maintained policies and procedures designed to promote and achieve compliance with such laws.

2.2 Bribery Act 2010 ("BA Act")

The Board of Idox is committed to zero-tolerance in relation to any form of bribery and corruption and sees the BA Act as part of its overall corporate responsibility. The Organisation will work to identify and eliminate any form of bribery through a risk assessment process and ongoing monitoring and review. All employees are prohibited from soliciting, arranging, offering, giving or accepting bribes intended for the business and / or employee's benefit or that of the employee's family, associates or acquaintances. This policy extends to the Organisation's business dealings and transactions in the UK and abroad, whether on its own behalf or on behalf of any business managed or operated, wholly or in part, by any Idox entity.

This policy is supported by a detailed anti-bribery programme which will be regularly revised to capture changes in law, reputation demands and changes in the business.

2.3 Constraints and Conflicts of Interest

As a publicly listed company with no links to the public sector other than commercial, the Organisation does not envisage any constraints on the provision of its services to the public sector. However, the Organisation understands that while working in a public sector environment there is the possibility of conflicts of interest being experienced by its employees, attempting to seek personal, family or community benefits as a result of opportunities presented to them during their work. The Organisation's policies of customer care, security and confidentiality protect the client to the extent that any breach of these policies is a clear breach of the employee's terms and conditions of employment and is thus an instantly dismissible offence.

3 Whistleblowing

3.1 About this Policy

- Idox is committed to conducting business with honesty and integrity and expect all staff to maintain high standards. Any suspected wrongdoing should be reported as soon as possible.
- This policy covers all employees, officers, consultants, contractors, volunteers, interns, casual workers and agency workers.
- This policy does not form part of any employee's contract of employment and may be amended it at any time.

3.2 What is whistleblowing?

- Whistleblowing is the reporting of suspected wrongdoing or dangers in relation to Idox activities. This includes bribery, facilitation of tax evasion, fraud or other criminal activity, miscarriages of justice, health and safety risks, damage to the environment and any breach of legal or professional obligations.

3.3 How a concern is raised

- Idox hopes that in many cases employees will be able to raise any concerns with a manager. However, where employees prefer not to raise it with a manager for any reason, an employee should contact the Chief Legal and Corporate Officer, Ruth Paterson or the CEO, David Meaden.
- Idox will arrange a meeting with the employee as soon as possible to discuss their concern. Employees may bring a colleague or union representative to any meetings under this policy. The attending companion must respect the confidentiality of the disclosure and any subsequent investigation.

3.4 Confidentiality

- Idox hopes that staff will feel able to voice whistleblowing concerns openly under this policy. Completely anonymous disclosures are difficult to investigate. If employees want to raise their concern confidentially, Idox will make every effort to keep the identity of the employee raising a concern secret and only reveal it where necessary to those involved in investigating the concern.

3.5 External Disclosures

- The aim of this policy is to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace. In most cases employees should not find it necessary to alert anyone externally.
- The law recognises that in some circumstances it may be appropriate for employees to report a concern to an external body such as a regulator. Idox strongly encourages employees to seek advice before reporting a concern to anyone external. Public Concern at Work operates a confidential helpline. Their contact details are at the end of this policy.

3.6 Protection and Support for Whistle-blowers

- Idox aims to encourage openness and will support whistle-blowers who raise genuine concerns under this policy, even if they turn out to be mistaken.

- Whistle-blowers must not suffer any detrimental treatment as a result of raising a genuine concern. If an employee believes that they have suffered any such treatment, that employee should inform the Chief Legal and Corporate Officer or CEO immediately. If the matter is not remedied an employee should raise it formally using our Grievance Procedure.
- Employees must not threaten or retaliate against whistle-blowers in any way. If an employee is involved in such conduct that employee may be subject to disciplinary action. In some cases, the whistle-blower could have a right to sue an employee personally for compensation in an employment tribunal.
- However, if Idox concludes that a whistle-blower has made false allegations maliciously, the whistle-blower may be subject to disciplinary action.
- UK employees: Public Concern at Work operates a confidential helpline. Their contact details are at the end of this policy.

3.7 Contacts

Chief Legal and Corporate Officer: **Ruth Paterson**

Chief Executive: **David Meaden**

Public Concern at Work

(Independent whistleblowing charity - UK only)

www.pcaw.co.uk

whistle@pcaw.co.uk

[Helpline 020 7404 6609](tel:02074046609)

4 Anti-slavery and Human Trafficking

Idox is committed to ensuring that there is no slavery, servitude, forced or compulsory human labour, abuse of power over vulnerable individuals, human trafficking or any other form of exploitation as contemplated by the Modern Slavery Act 2015 ('**MSA**') in any part of Idox business or in the supply chain. In Idox policies, due diligence, contractual arrangements, training and reporting regimes, the Organisation is implementing and enforcing effective systems and controls to ensure that slavery and human trafficking are not taking place in any part of our business or in our supply chain.

The Chief Legal & Corporate Officer works in conjunction with the Supplier Chain Manager, Legal, Bids and People@Idox teams to help ensure compliance with the MSA. The Organisation is responsible for ensuring employees are paid fairly and properly for their work and developing systems and controls that safeguard against slavery and human trafficking taking place anywhere in our business or supply chains.

The Organisation has adopted a risk-based approach to the assessment of our business and supply chain through our supply chain management policy, which has involved taking geographical, industry and market factors into account in order to identify categories of supply that may present a higher risk of modern slavery being present. We are focusing attention on suppliers in these category areas initially, although any resulting policy changes will extend to the whole business. Given the nature of what we do, we believe that there is a low risk of slavery or human trafficking having a connection with our business activities.

The main mitigations to ensure Idox remains an anti-slavery business include:

- Ensuring our employees receive a fair wage.
- Supporting whistleblowing.
- Requiring compliance with our ethical conduct policy.
- Recruitment checks and supplier checks.

The Organisation sees diversity as a strength, and we are committed to respecting each individual's human rights and we provide equal opportunities to all qualified employees and applicants.

- An annual statement is made pursuant to section 54(1) of the MSA and constitutes the Organisation's slavery and human trafficking statement for each financial year. This statement is available to view on the Idox website.

5 Fraud Prevention

Idox has a zero-tolerance approach to fraud and is committed to fostering an anti-fraud culture by developing robust systems and controls to prevent fraud across all aspects of the Organisation's business.

In line with the Fraud Act 2006 and other relevant statutory instruments, Idox is dedicated to preventing any form of fraud within its operations. The Organisation's policies, due diligence procedures, contractual arrangements, training programmes and reporting mechanisms are designed to implement and enforce effective systems and controls. These measures ensure compliance with legal requirements and counter the risk of Idox or its customers becoming targets or facilitators of fraudulent activity.

To mitigate the risk of both internal and external fraud, Idox has implemented several key measures, including but not limited to:

- Providing employee training on fraud awareness and prevention;
- Encouraging and supporting whistleblowing to report suspicious activities;
- Conducting regular fraud risk assessments to identify potential vulnerabilities;
- Monitoring and analysing fraud trends to stay ahead of emerging threats;
- Investing in advanced anti-fraud systems and technologies;
- Implementing robust internal controls and procedures to prevent fraudulent activities.

6 Occupational Health and Safety

The Organisation remains aware of its responsibilities relating to Occupational Health and Safety ('**OH&S**') matters throughout its business activities.

By Management review and staff training, the Organisation ensures that its performance relating to OH&S matters is subject to continual improvement.

The Organisation complies with all OH&S legislation and regulations applicable to its activities and to any other requirements to which the Organisation may subscribe, in particular in relation to the supply of specialist information management software solutions and services.

This OH&S Policy, held separately as part of the Health & Safety System, is maintained by regular review and is communicated to all of the Organisation's employees, suppliers and sub-contractors.

This OH&S Policy is made available to all interested parties including members of the general public.

This OH&S Policy is subject to regular Management review in order to ensure that it remains relevant and appropriate to the Organisation's activities.



7 Equality and Diversity

Idox is committed to providing equal opportunities in all aspects of employment particularly recruitment, promotions and training.

Idox will provide equal opportunities to any employee or job applicant and will not discriminate either directly or indirectly on the grounds of age, race, colour, nationality, gender, sexual orientation, religion or marital status. Disabilities will be accommodated wherever practicable. Idox also affirms its commitment to treat part-time staff and contract workers as equitably as full-time staff, having regard to statutory obligations.

To meet these objectives Idox will ensure that:

- Selection criteria relating to job requirements are defined to attract the widest possible pool of suitably qualified candidates and not discriminatory.
- Job descriptions and personnel specifications are not discriminatory.
- Job advertisements are not, without proper reason, confined only to certain publications, or worded in such a way as to exclude applicants either individually or of a particular group.
- Job advertisements will carry a statement that the Organisation is an Equal Opportunities Employer.
- Every job is open equally to all applicants who meet the job requirements.
- Applications will be dealt with in accordance with appropriate procedure (See Code of Practice).
- Transfer, promotion and training are all open equally to all eligible employees and selection criteria do not exclude applicants from any group.
- Recruitment, selection and employment policies will be periodically reviewed, and a detailed Code of Practice will be available to implement the Equal Opportunities Policy.

7.1 Code of Practice

The Organisation will not tolerate:

- Discrimination, whether direct or indirect;
- Harassment;
- Victimisation;
- Instructing, causing or inducing others to do anything that contravenes the Equality Act 2010; or
- any other unlawful conduct prohibited by the Equality Act 2010,
- on any of the following grounds: age, disability, gender assignment, sex, marital status, pregnancy and maternity, sexual orientation, race (including colour, nationality, ethnic or national origin), religion or belief, or membership or non-membership of a trade union (**Protected Characteristics**).

The Organisation will not tolerate, in particular, discrimination on the ground of any Protected Characteristics, including:

- By expecting an individual to comply with requirements for any reason whatsoever related to their employment, which are different to the requirements for others;

- By imposing work that is more onerous on one employee than on others; or
- By any other act or omission, which has the effect of disadvantaging an employee or applicant with a particular Protected Characteristic.

It is the policy of the Organisation to ensure that entry into the Organisation is determined solely by the application of objective criteria and individual merit. Equality will be accorded to applicants and employees without regard to their Protected Characteristics save as permitted by the Equality Act 2010.

The objective of the Organisation is to employ individuals who are suitably qualified or who have the ability to develop the skills necessary to undertake the obligations imposed by the position they occupy.

7.2 Management Responsibility

The Chief Executive Officer has overall responsibility to ensure this policy is consistently applied and each manager has responsibility for the implementation of the policy in his or her area.

The Organisation has implemented the following measures to ensure that no discrimination or other unlawful conduct occurs:

- Those with responsibility for staff are reminded that they may be held individually accountable for ensuring that no form of discrimination occurs in the recruitment, selection, promotion, training and discipline of these staff.
- Enquiries will be made into suspected cases of discrimination or other unlawful conduct under the Equality Act 2010. Any such practices will be stopped, and disciplinary action may be taken against the individuals concerned.
- The Executive Management Team has the responsibility for ensuring that the relevant provisions of this policy on discrimination and other unlawful conduct are set out:
 - In instructions to those concerned with recruitment, training, promotion, employee management in relation to disciplinary actions or employee grievances;
 - In documents available to employees, recognised trade unions or other representative groups of employees;
 - In recruitment advertisements or other literature;
 - In accessible formats for disabled employees, applicants or customers (if applicable);
 - In instructions or procedures for employees involved with service delivery, customer care and procurement of services and goods;
 - In relevant documents relating to sub-contractors used or employed.

8 Security and Confidentiality

The Organisation is committed to the highest standards of information security, at present we are accredited to ISO 27001:2022 standard. Underpinning this commitment is the Idox Information Security Policy which applies to all business functions and covers the information, information systems, networks, physical environment and people supporting these business functions.

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:

- **Confidentiality** and protection against unauthorised disclosure.
- **Integrity** of information including protection against unauthorised or accidental modification.
- **Availability** as and when required in pursuance of the Organisation's business objectives.

The board of Idox regularly reviews the implementation of Cyber Security, Data Integrity, Data Protection within the Organisation.

8.1 Confidentiality Policy

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 in a project are briefed about any special security or confidentiality agreements. The PM should also remind staff about this policy at the beginning of each project 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 a client's agreements or the Idox standard agreement.

8.2 Data Protection Policy

8.2.1 Policy Statement

The Organisation provides a range of software, research, content management, and delivery solutions across on site, hosted, and cloud environments to its clients.

The personal data that the Organisation processes to provide these services relates to its clients and other individuals as necessary, including employees and suppliers' employees and other third parties.

This policy sets out the Organisation's commitment to ensuring that any personal data, including special category personal data, which the Organisation processes, is processed in compliance with Data Protection Law (as defined below in this section). The Organisation processes the personal data of employees in a number of jurisdictions, including the personal data of non-EU citizens, but is committed to ensuring that all the personal data that it processes is done in accordance with Data Protection Law. The Organisation ensures that good data protection practice is embedded in the culture of the Organisation.

The Organisation operates and maintains a number of other information security policies and processes which support and strengthen its data protection commitments. These include but are not limited to:

- Record of Processing Activities
- Information Asset Register
- Privacy notices (website, clients, employees)
- Incident Management Policy (encompassing Personal Data Breach reporting)
- Record Retention Policy
- Data Protection Impact Assessment process (DPIA)

'**Data Protection Law**' includes the UK GDPR as defined in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018; the Data Protection Act 2018 and all relevant EU and UK data protection legislation in force from time to time.

Further information on legislation affecting our Organisation's data use can be found within the Applicable Legislation Register.

8.2.2 Scope

This Policy applies to all employees of the Organisation.

For the purpose of this Policy the term 'Employee' refers to all full-time and part-time employees, temporary employees, agency workers, contractors and consultants.

All employees must read, understand and comply with this Policy when processing personal data on the Organisation's behalf and complete information security training provided.

8.2.3 Data protection principles

The Organisation is committed to processing data in accordance with its responsibilities under Data Protection Law.

Article 5 of the UK GDPR requires that personal data shall be:

- a. processed lawfully, fairly and in a transparent manner in relation to individuals.
- b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

- c. adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

8.2.4 General provisions

- a. This policy applies to all personal data processed by the Organisation.
- b. The Data Protection Officer (DPO) shall take responsibility for the Organisation’s ongoing compliance with this policy.
- c. The Organisation shall register its relevant data processing and data controlling operations with the Information Commissioner’s Office.

8.2.5 Lawful, fair and transparent processing

- a. Personal data must be processed lawfully, fairly and in a transparent manner in relation to data subjects.
- b. To ensure its processing of data is lawful, fair, and transparent, the Organisation shall maintain a Register of Processing Activities.
- c. The Register of Processing Activities shall be reviewed at least annually.
- d. Individuals have the right to access their personal data and any such requests made to the Organisation shall be responded to within the statutory time limits in the Data Protection Laws.
- e. At point of collection, where personally identifiable information is collected, the Organisation will provide clear, concise, transparent, intelligible, and easily accessible Privacy Notices for the Data Subject.
- f. The Organisation will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless it has informed the data subject of the new purposes and they have Consented where necessary.

8.2.6 Lawful purposes

- a. All data processed by the Organisation must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task, or legitimate interests ([see ICO guidance for more information](#)).
- b. The Organisation shall note the appropriate lawful basis in the Register of Processing Activities.
- c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

- d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Organisation's systems.

8.2.7 Data minimisation

- a. The Organisation shall ensure that personal data which it processes is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- b. Employees of the Organisation must only process personal data when their job duties require it. Employees cannot process personal data for any reason unrelated to their job duties.

8.2.8 Accuracy

- a. The Organisation shall take reasonable steps to ensure personal data is accurate and is kept for no longer than is necessary for the purpose in which the personal data is processed.
- b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

8.2.9 Archiving / removal

- a. To ensure that personal data is kept for no longer than necessary, the Organisation shall put in place a Record Retention Policy for each area in which personal data is processed and review this process annually.
- b. The Record Retention Policy shall consider what data should/must be retained, for how long, and why.

8.2.10 Security

- a. The Organisation shall ensure that personal data is stored securely by using appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.
- b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- c. When personal data is deleted, this should be done safely such that the data is irrecoverable.
- d. Appropriate back-up and disaster recovery solutions shall be in place.
- e. Employees of the Organisation are provided with mandatory annual data protection training to ensure they are aware of the level of care which personal data must be treated with.

8.2.11 Sub-processing

Where third parties are used to process personal data on behalf of the Organisation, responsibility for the security and appropriate use of that data remains with the Organisation.

Where a third-party data processor is used:

- a) a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- b) reasonable steps must be taken that such security measures are in place;
- c) a written contract establishing what personal data will be processed and for what purpose must be set out;
- d) a data processing agreement, available from the Organisation's legal team, must be signed by both parties.

For further guidance about the use of third-party data processors please contact the Organisation's Information Governance team.

8.2.12 Data Sharing

The Organisation will not share Personal Data with any third parties unless certain safeguards and contractual arrangements have been put in place.

In the absence of a lawful basis for processing, personal data will not be disclosed to third parties unrelated to the Organisation.

In the event that the Organisation is required to share personal data with a third party and a lawful basis for this sharing exists, personal data will only be shared if certain safeguards and contractual arrangements are in place including if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the personal data complies with the Organisation's privacy notice provided to the data subject and, if required, the data subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross-border transfer restrictions; and
- a fully executed written data processing agreement that contains UK GDPR-approved third party clauses has been obtained.

8.2.13 Subject Access Requests (SARs)

The Organisation will respect the rights of data subjects, including the right to access, rectify, erase, restrict processing, object to processing, and data portability.

The Organisation will respond to subject access requests, replying as quickly as possible, and in any event within the 1-month time limit. Whilst individuals have a general right of access to any of their own personal information, which is held, the Organisation will be mindful of those circumstances where an exemption may apply.

Where subject access requests may infringe on another data subject's right to privacy, the Organisation will always endeavour to seek the permission of the data subject or redact such information to protect the individual.

8.2.14 Responsibility for the processing of personal data

The directors of the Organisation take ultimate responsibility for data protection.

If you have any concerns or wish to exercise any of your rights under Data Protection Law, then you can contact the data protection lead in the following ways:

Name: Idox Plc (Privacy)

Address: Unit 5, Woking 8, Forsyth Road, Woking, Surrey, GU21 5SB

Email: privacy@idoxgroup.com

Telephone: +44 (0) 333 011 1200

8.2.15 Personal Data Breaches

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Organisation shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO and the Data Subject([more information on the ICO website](#)).

If an Employee knows or suspects that a personal data breach has occurred, they should not attempt to investigate the matter themselves. Instead, they should ensure that all evidence relating to the potential personal data breach is preserved and follow the procedure for reporting the event, outlined within the Organisation's Incident Management Policy.

8.2.16 Monitoring and review

This policy shall be regularly monitored and reviewed, at least annually.

8.2.17 Enforcement

Failure of an employee to comply with this policy may lead to the instigation of disciplinary procedures and, in certain circumstances, legal action may be taken.

Failure of a contractor or third-party processor to comply may lead to the immediate cancellation of a contract and possible legal action. Where appropriate, breaches of the law will be reported to the relevant authorities.

8.3 Information Security Policy

8.3.1 Purpose

The purpose of this document is to provide a description of the aims, objectives, and overall structure of the Information Security Management System.

8.3.2 Scope

This Policy applies to all business functions within the scope of the Information Security Management System and covers the information, information systems, networks, physical environment (including cloud based and directly hosted services) and products and services. The Policy applies to all employees, contractors and third parties supporting these business functions.

8.3.3 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:

- **Confidentiality**, i.e. protection against unauthorised disclosure
- **Integrity**, i.e. protection against unauthorised or accidental modification
- **Availability** as and when required in pursuance of the Organisation's business objectives
- **Authentication**, i.e. the assurance that the data, transactions, communications or documents (electronic or physical) are genuine
- **Non-repudiation**, i.e. the assurance of proof of origin and integrity of data.

8.3.4 Responsibilities

CEO:	Overall responsibility for Information Security. Responsible for ensuring that the appropriate levels of resources are made available to support the Information Security function.
Management:	Ensure their employees and contractors comply with this Policy.
Information Security Manager:	Operational responsibility for procedural matters, legal compliance, maintenance and updating of documentation, promotion of security awareness, liaison with external organisations, incident investigation and management reporting.
Data Protection Officer:	Day-to-day responsibility for data protection.
IT Staff:	Responsibility for technical matters, including technical documentation, systems monitoring, technical incidence investigation and liaison with technical contacts at external organisations.
Employees and contractors:	Responsibility for safeguarding assets, including locations, hardware, software, systems or information in their care and to report any suspected breach in security.

8.3.5 Principles

The Information Security Policy is the means by which the Organisation meets the requirements

of ISO/IEC 27001:2022 relating to its business risks. It specifies the requirements for the implementation of appropriate security controls to meet identified risks relating to the activities of the Organisation.

The implementation and continuing control of this system are fundamental to all work undertaken by the Organisation. The procedures established are adopted and practiced by all employees at every level.

The Organisation has adopted the process approach for developing, implementing and improving the effectiveness of its ISMS.

The Organisation, in adopting the process approach is committed to:

- Understanding business information Security requirements and the need to establish Policies and Objectives for Information Security
- Implementing and operating controls in the context of managing the Organisation 's overall business risk
- Monitoring and reviewing the performance and effectiveness of the ISMS
- Continual improvement based on objective measures
- Communicating throughout the Organisation the importance of meeting all relevant statutory and regulatory requirements specifically related to its business activities
- Ensuring that adequate resources are determined and provided to monitor and maintain the ISMS.

8.3.6 Information Security

Information Security aspects are taken into account in all daily activities, processes, plans, projects, contracts and partnerships entered into by the Organisation.

Awareness and compliance to Information Security procedures as set out in the various Policies and guideline documents are a requirement of employees and a clause to this effect is set out in the Contracts of Employment.

Copies of all Information Security Policies are made available to all employees.

Breach of the Information Security Policies and procedures by employees may result in disciplinary action, including dismissal.

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.

A Business Continuity Plan is in place. This is maintained, tested and subjected to regular review.


Statutory and regulatory requirements are met and monitored for ongoing changes.

Further Policies such as those for access, acceptable use of email and the Internet, malware protection, backups, passwords, systems monitoring etc. are in place, maintained and are regularly reviewed.

This Information Security Policy is reviewed at least annually 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 Management Systems.

The ISMS and Information Security operations are subject to continuous improvement through a program of internal and external audits and risk assessments.

Non-disclosure/Confidentiality Agreements are entered into as appropriate with third party companies.

Date of Issue: 20 June 2024	Signed: 
Date of Next Review: 1 June 2025	Print Name: TIM STRINGER Director of Information and Security



Certificate No.263672020



Certificate No.180572021

9 Environmental Safety

9.1 Environmental Policy Objectives

The Organisation recognises the importance of environmental protection and is committed to operating its business responsibly and in fulfilment of its compliance obligations relating to the supply of software solutions and information services to the public sector and increasingly to highly regulated asset intensive industries around the world in the wider corporate sector. It is the Organisation's declared policy to operate with and to maintain good relations with all regulatory bodies.

It is the Organisation's objective to carry out all measures reasonably practicable to meet, exceed or develop all necessary or desirable requirements, to protect the environment and to continually improve the Environmental Management System to enhance environmental performance through the implementation of the following:

1. Assess and regularly re-assess the environmental effects of the Organisation's activities
2. Training of employees in environmental issues
3. Minimise the production of waste
4. Minimise material wastage
5. Minimise energy wastage
6. Promote the use of recyclable and renewable materials
7. Prevent pollution in all its forms
8. Control noise emissions from operations
9. Minimise the risk to the general public and employees from operations and activities undertaken by the Organisation.

Top management demonstrates leadership and commitment with respect to the Environmental Management System by:

1. Taking accountability for the effectiveness of the Environmental Management System
2. Ensuring that the Environmental Policy and Environmental Objectives are established and are compatible with the strategic direction and the context of the Organisation
3. Ensuring the integration of the Environmental Management System requirements into the Organisation's business processes
4. Ensuring that the resources needed for the Environmental Management System are available
5. Communicating the importance of effective environmental management and of conforming to the environmental management system requirements
6. Ensuring that the Environmental Management System achieves its intended outcomes.
7. Directing and supporting persons to contribute to the effectiveness of the environmental management system
8. Promoting continual improvement


- 9. Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

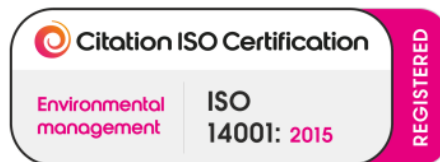
This Policy is communicated to all employees and whenever it is considered relevant to the goods or services required, a copy of the Organisation’s Environmental Policy is issued to all suppliers and sub-contractors.

Suppliers and sub-contractors are subject to a review of their environmental performance as part of the approval process before being appointed as approved suppliers.

9.2 Environmental Management System Accreditation

Idox Software Ltd is accredited to BS EN ISO 14001:2015 which encompasses this Policy and the Environmental Management System.

Date of Issue: 20 June 2024	Signed: 
Date of Next Review: 19 June 2025	Print Name: David Meaden



Certificate No:123912021

10 Inside Information and Share Dealing

In the course of employment with the Organisation, directors and employees become aware of information about Organisation or other companies that has not been made public. The use or disclosure of such non-public or "inside" information about Idox or another company for financial or other benefit is not only unethical, but also it may be a violation of the Market Abuse Regulation applicable in the UK and across the EU. These laws make it unlawful for any person who has "material" non-public information about a company to trade the shares of that company. Violation of such laws may result in civil and criminal penalties, including fines and jail sentences. The Organisation will not tolerate the improper use of inside information. These prohibitions also apply anywhere in the world where we do business. All employees are to comply with the Organisation Share Dealing Policy.

Idox Share Dealing Policy (Adopted on 1 July 2016)

- This policy applies to all directors and employees of Idox plc (the '**Company**') and its subsidiaries. It has been designed to ensure that directors and employees do not misuse, or place themselves under suspicion of misusing, information about the Organisation which directors and employees have, and which is not public.
- Directors and employees must not deal in any securities of the Organisation if directors and employees are in possession of inside information about the Organisation. Directors and employees also must not recommend or encourage someone else to deal in the Organisation's securities at that time – even if directors and employees will not profit from such dealing.
- Directors and employees must not disclose any confidential information about the Organisation (including any inside information) except where required to do so as part of employment or duties. This means that directors and employees should not share the Organisation's confidential information with family, friends or business acquaintances.
- Directors and employees may, from time to time, be given access to inside information about another group of companies (for example, one of the Organisation's customers or suppliers). Directors and employees must not deal in the securities of that group or companies at those times.
- The Organisation also operates a Dealing Code which applies to the Company's directors and to employees who are able to access restricted information about the Organisation (for example, employees who are involved in the preparation of the Organisation's financial reports and those working on other sensitive matters). Directors and employees will be told if they are required to comply with the Dealing Code. Directors and employees who are required to comply with the Dealing Code must also comply with this policy.
- Failure to comply with this policy may result in internal disciplinary action. It may also mean that directors and employees have committed a civil and/or criminal offence.
- If directors and employees have any questions about this policy or are not sure whether they can deal in securities at any particular time, please contact the Company Secretary.

Online document links:

[Idox Securities Dealing Code for Restricted Persons](#)

[Idox Securities Dealing Procedures Manual](#)

11 Contact us

Idox Software Ltd

Unit 5, Woking 8
Forsyth Road
Woking
Surrey

T: +44 (0) 333 011 1200
E: info@idoxgroup.com
www.idoxgroup.com