	ISDL No:	ISDL390	Version:	4.0	Class:	Public
	Title:	Statutory, Regulatory, and Contractual Requirements Policy				

Access Intelligence Statutory, Regulatory and Contractual Requirements Policy

1.0 *Policy Objectives*

To ensure that Access Intelligence can operate a trusted, established Information Security Management System, it shall:

- Identify all requirements, whether legislative, regulatory, contractual or otherwise relevant to achieving the above and the lawful functioning of the business; and
- Maintain compliance with all applicable requirements for the duration (and thereafter, where required) of Access Intelligence's operations.


2.0 *Policy Scope*

Access Intelligence Statutory, Regulatory and Contractual Requirements Policy shall include the following:

- This Policy shall apply to all employees, contractors and third-party users of Access Intelligence's information systems, and other related infrastructure.
- All applicable laws, regulations and contractual requirements
- All information assets (data) owned by Access Intelligence
- All information assets (data) belonging to a client or a third party entrusted to Access Intelligence under an agreement which specifically details Access Intelligence's responsibility for the security of that data
- The selection, implementation and effectiveness of controls used to manage statutory, regulatory and contractual compliance.

3.0 *Policy Statements*

The laws which apply to any given organisation are extensive. This is intensified by the UK's evolving relationship with Europe and the general pace of socio-economical change (including technological advancement) which is continuously influencing the legal system of England and Wales. Although it is not practically possible to provide an exhaustive list of statutory requirements, Access Intelligence shall maintain compliance with the laws of England and Wales (including the European Union to the extent that such laws are binding and/or codified into UK legislative Acts of Parliament) including but not limited to:

	ISDL No:	ISDL390	Version:	4.0	Class:	Open
	Title:	Statutory, Regulatory, and Contractual Requirements Policy				

General

- GDPR (both EU and UK equivalent)
- Data Protection Act 2018
- Privacy Electronic Communications Regulations (PECR)
- The Privacy and Electronic Communications Directive 2003
- Freedom of Information Act 2000
- Limitation Act 1980
- Malicious Communications Act 1988
- Electronic Communications Act 2000
- Electronic Identification Regulations 2016
- Communications Act 2003
- The Environment Act 2021

Commercial

- Copyright, Designs and Patents Act 1988
- Trademarks Act 1994
- Trade Secrets (Enforcement Etc.) Regulations 2018
- Competition Act 1998

Accounting and Finance


- Financial Reporting Codes and Guidance Act 2013
- Finance Act
- Fraud Act 2006
- Bribery Act 2010
- The Sanctions and Anti-Money Laundering Act 2018

Corporate

- AIM Company Rules
- Nominated Advisor Rules
- London Stock Exchange Rules for member firms
- Company Constitution (AoA)
- City Code (takeovers and mergers)

Human Resources

- Employment Rights Act 1996
- Employment Act
- Health & Safety at Work Act 1974
- Human Rights Act 1998
- Equality Act 2010
- Modern Slavery Act 2015

 accessintelligence	ISDL No:	ISDL390	Version:	4.0	Class:	Open
	Title:	Statutory, Regulatory, and Contractual Requirements Policy				

Access Intelligence shall organise training for those of its employees and contractors whose responsibilities are dependent upon adherence to laws specific to a departmental function (i.e.: Legal, Finance, Human Resources etc.)

All training described in this Statutory, Regulatory and Contractual Requirements Policy shall be provided during the induction of new staff and, at a minimum, yearly thereafter.

When hiring for such roles, Access Intelligence shall ensure that reasonable familiarity with applicable laws and regulations proportionate to the role being hired for (including verification of any professional certifications) is a pre-requisite to the recruitment of an employee.

Access Intelligence shall engage the assistance of 3rd party professionals to objectively evaluate and advise on Access Intelligence’s standard of compliance with statute, regulation and relevant contractual obligations.


As part of Access Intelligence’s annual review of all ISMS policies, Access Intelligence shall review its Information Security Management System to ensure that it’s policies and processes are aligned with all legislative, regulatory and contractual commitments.

Access Intelligence shall ensure that all information systems and security protocols initiated by the Access Intelligence Information Security Management System are regularly reviewed, audited and updated to remain in compliance with applicable law, regulation and contractual requirements.

Access Intelligence shall communicate all relevant legal, contractual and statutory requirements to all staff through internal policies and codes of conduct.

Access Intelligence shall comply with its contractual commitments by:

- Appropriate storage, record and accessibility of all contracts through CRM and other systems;
- Debriefing all employees and contractors of Access Intelligence’s contractual duties as applicable to specific roles through training;
- Ensuring all employment contracts contain obligations which sufficiently address confidentiality, intellectual property rights and data protection;
- Maintaining compliance with its ISMS and all associated policies as part of the Information Security Document Library.
- Ensuring that any third-party contractor who is delegated any contractual responsibility is subject to the same duties as Access Intelligence.

 accessintelligence	ISDL No:	ISDL390	Version:	4.0	Class:	Open
	Title:	Statutory, Regulatory, and Contractual Requirements Policy				

4.0 ***Responsibilities***

Within Access Intelligence, all employees, contractors and third-party users shall understand their role in compliance with all legislative, regulatory and contractual requirements through the mechanisms set out in Section 3.0 above.

There are, however, additional responsibilities defined in order that the ISMS shall operate efficiently and in accordance with the requirements of statute, regulation and contractual obligations. These are as detailed in Section 4 of the Information Security Policy (**ISDL01**).


The Access Intelligence Legal Team shall be responsible for:

- Working with Department/Function Managers to identify and implement processes to align with applicable laws, regulations and contractual duties;
- Providing regular updates through the meetings described in the Access Intelligence Management Review Policy (**see ISDL09**) of new/emerging legislation and impact on Access Intelligence's Information Security Management System;
- Assisting in the facilitation of all training;
- Reviewing/updating the Information Security Management System along with any internal contractual templates to ensure compliance; and
- Liaising with external legal professionals for the purposes of training, knowledge sharing and generalist advice on day to day business matters as well as company-wide projects.

The Data Protection Officer shall be responsible for:

- Maintaining awareness of data protection regulations
- Organising awareness training for all staff
- Assisting the Legal Team by facilitating activities

All individuals specified within the Policy Scope of this Statutory, Regulatory and Contractual Requirements Policy (see section 2.0) shall have individual responsibility for complying with every aspect of this policy. The requirement to comply with Access Intelligence policies is included within the Terms and Conditions of Employment and is noted within each individual user's job description. Any failure to adhere to the requirements of this policy shall result in disciplinary action being taken.

	ISDL No:	ISDL390	Version:	4.0	Class:	Open
	Title:	Statutory, Regulatory, and Contractual Requirements Policy				

5.0 Document Version Control

This policy needs to be reviewed annually as an absolute minimum, or if required changes are identified to address one or more of the following:




- An identified shortcoming in the effectiveness of this policy, for example because of a reported information security incident, formal review or audit finding.
- A change in business activities (e.g. mergers and acquisitions) which will or could possibly affect the current operation of the Access Intelligence Information Security Management System, and the relevance of this document.
- A change in the way in which Access Intelligence manages or operates its information assets and/or their supporting assets, which may affect the validity of this document.

The current version of this policy, together with its previous versions, shall be recorded below:

Version History

Revision	Author	Date	Reason for issue
1.0	Lakhan Shah	13/02/2020	First issue to form part of ISMS mandatory document set in readiness for ISO 27001 accreditation
2.0	Lakhan Shah	18/01/2021	Updated to reflect change in data privacy practices.
3.0	Lakhan Shah	09/12/2021	Annual policy review
4.0	Adam Palmer	05/01/2023	Included regulations to support social and environmental responsibilities

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer		18/01/2021
Mark Fautley	Chief Financial Officer		20/01/2022
Mark Fautley	Chief Financial Officer		19/01/2023