Access Intelligence Information Security Policy

1.0 Policy Objectives

- To direct the design, implementation and management of a coherent and consistent Information Security Management System (ISMS), which ensures that Access Intelligence's information assets are adequately identified, always recorded and afforded suitable protection.

- To ensure the confidentiality, integrity and availability of Access Intelligence's information assets and supporting assets (including information systems) as defined within the Inventory of Assets.

- To ensure that all vulnerabilities, threats and risks to information assets and supporting assets are formally identified, understood, assessed and controlled in accordance with Access Intelligence's documented Risk Assessment Methodology.

- To ensure that Access Intelligence's employees, contractors and third-party users comply with this Information Security Policy, and all other ISMS documentation, through the provision of effective information security training, awareness and ongoing monitoring activities.

- To ensure that Access Intelligence can maintain full compliance with all applicable legislation, regulations and contractual requirements, and any supporting management system certifications (e.g. ISO/IEC 27001:2013)

2.0 Policy Scope

Access Intelligence's Information Security Policy shall include the following:

2.1 Information Assets

All information assets (data) either owned by Access Intelligence or entrusted to Access Intelligence by a client under an agreement which specifically details Access Intelligence's responsibility for that data and including:

- Information assets held, processed or stored on Access Intelligence's premises
- Information assets held, processed or stored at approved off-site premises or locations

2.2 Supporting Assets

All supporting assets (non-data) which by direct or indirect association are an integral part of ensuring the confidentiality, integrity or availability of the information assets described in Section 2.1, including:

- Premises (including offices, data centres, storage facilities, recovery sites).
- Hardware (including servers, network infrastructure, laptop computers, desktop computers, storage infrastructure and mobile devices).
- Software (including operating systems, commercially available software applications and software applications developed internally by Access Intelligence).
- Access Intelligence personnel (including permanent, temporary, full-time and part-time employees, authorised contractors and any third-party users of information systems).

2.3 Documentation and Records

All policies, processes, procedures, work instructions and records related to the management, use, control and disposal of the information assets and their supporting assets detailed above.

3.0 Policy Statements

Access Intelligence shall be committed to the protection of the information assets and supporting assets as defined within the Scope of this Policy. Access Intelligence has created its Information Security Management System (ISMS) in accordance with the international Information Security Management Systems standard ISO/IEC 27001:2013 this framework shall be followed for all information security related activities, and Access Intelligence shall seek to acquire and maintain external certification against this standard.

After reviewing the needs and expectations of interested parties, the scope of the ISMS (**see ISDL325**) was defined to support these requirements.

To effectively manage and deliver its ISMS, Access Intelligence shall:

3.1 Inventory of Assets

Define and maintain a comprehensive Inventory of Assets, including all information assets and supporting assets as defined within Section 2.0 of this Policy. The Inventory of Assets shall detail a named owner for each asset, who shall fully understand their responsibilities for the protection of the asset in accordance with the documented Access Intelligence Asset Management Policy (**see ISDL05**).

3.2 Access Control

Ensure that all information assets, and their supporting assets, are protected with strong passwords in accordance with the Access Intelligence Password Management Policy (**see ISDL03**) and to ensure their confidentiality, integrity and availability is maintained. Access to information assets and supporting assets shall be in accordance with Access Intelligence's Access Control Policy (**see ISDL07**) and be restricted to the minimum required to undertake authorised business activities, and Access Intelligence has adopted the principle that "access is forbidden unless it has been specifically and formally pre-authorised".

3.3 Information Classification and Handling

Ensure that all information assets shall be classified and handled in accordance with the Access Intelligence Information Classification and Handling Guide (see **ISDL52**), which details how information assets of different sensitivities shall be managed, handled, processed, encrypted, stored, transmitted, dispatched and disposed of when no longer required. This Guide also details the appropriate levels of personnel screening or clearances necessary to access information of different classifications.

3.4 Acceptable Use

Ensure that all personnel, contractors and third-party users comply with Access Intelligence's Acceptable Use Policy (**see ISDL06**) which describes how information assets and their supporting assets should be used in an acceptable manner and in accordance with

all ISMS related policies and processes. This policy shall describe the acceptable methods of use of information processing systems, networks (including, for example, the internet and telephone systems) and other resources within the scope of this policy.

3.5 Risk Assessment

Perform regular risk assessments on all information assets, and their supporting assets, as detailed within Access Intelligence's Risk Assessment Methodology (**see ISDL31**) and using the control objectives and controls as documented within Annex A of ISO/IEC27001:2013. The documented results of risk assessments shall be reviewed to understand the level of risk to information and supporting assets, and appropriate controls applied as appropriate to address any unacceptable risks that have been identified. A Statement of Applicability (SoA) shall be produced to record which controls have been selected and the reasons for their selection, and the justification for any controls not selected.

3.6 Information Security Incidents

Provide a mechanism for the swift identification, reporting, investigation and closure of information security incidents to Access Intelligence, in accordance with the Information Security Incident Policy (**see ISDL04**), and to fully analyse reported incidents to identify the root cause of issues and take advantage of any improvement opportunities which may have been identified.

3.7 Business Continuity Management

Ensure that information security is a key consideration within the Business Continuity Management Policy (**see ISDL08**) so that the security of Access Intelligence's information assets is not compromised even when faced with a wide variety of unplanned business interruptions.

3.8 Information Security Training

Develop a regular training and education programme, in accordance with the Information Security Training Policy (**see ISDL02**), which shall be mandatory for all Access Intelligence's employees, contractors and third-party users, which details their individual responsibilities to fully comply with the requirements of the ISMS policies, processes and work instructions defined within Section 2.0 of this policy.

3.9 Management, Monitoring and Review

Continually monitor, review and improve the Access Intelligence ISMS, in accordance with the Management Review Policy (**see ISDL09**), by undertaking regular reviews, internal audits (in accordance with the Internal Audit Policy **ISDL14**) and other related activities, and taking prompt corrective actions and implementing improvement opportunities in response to the findings of these activities.

3.10 Legislative Compliance

Ensure consistently that its Information Security Management System shall support full compliance with the requirements of the UK and EU GDPR (in accordance with the Data Protection Policy **ISDL13**) and other UK legislation and regulations (in accordance with the Statutory Regulatory and Contractual Compliance Policy **ISDL390**), including but not limited to:

- UK and EU General Data Protection Regulations ("GDPR")
- Data Protection Act 2018
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Companies Act 2006
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Waste Electrical and Electronic Equipment Directive (WEEE) 2003
- PCI-DSS Payment Card Industry Data Security Standard (if applicable)
- FCA Requirements

3.11 Change Control

Minimise risks during development by improving security controls for people and technology, in accordance with the Data Encryption Policy (**see ISDL11**), Secure Development Policy (**see ISDL77**) and Change Management Policy (**see ISDL54**), so that the security of Access Intelligence's information assets is not compromised, even in an ever-changing cloud environment.

3.12 Supplier Security

Ensure that sufficient security controls and agreements are in place to protect Access Intelligence's assets that are accessible by suppliers, in accordance with the Supplier Security Management Policy (**see ISDL19**). The policy shall describe what requirements must be adhered to when engaging third parties, the standard terms that should be included in supplier agreements and how Access Intelligence will monitor compliance.

3.13 People Security

Minimise risk in the workforce by implementing security controls pre-employment in accordance with the Access Intelligence ISMS Employee Screening Policy (**see ISDL55**) and by including Information Security responsibilities into job descriptions (**see ISDL53**).

3.14 Device Security

Reduce risk of information leakage by only working on devices provided and managed by the organisation or for specific processes as per the Access Intelligence ISMS Mobile and Personal Device Policy (**see ISDL30**). When unattended, devices must be locked, and no information should be displayed on the workstation as per the Access Intelligence ISMS Clear Desk and Clear Screen Policy (**see ISDL16**).

4.0 ISMS Responsibilities

4.1 Employees, Contractors and Third-Party Users

Within Access Intelligence, all information security responsibilities are defined and allocated in accordance with the Roles and Responsibilities Policy (**see ISDL10**). All employees, contractors and third-party users shall understand their role in ensuring the security of information assets (and their supporting assets) in accordance with the Information Security Training Policy (**see ISDL02**) as detailed in Section 3.0.

There are, however, additional responsibilities defined in order that the ISMS shall operate efficiently and in accordance with the requirements of ISO/IEC 27001:2013. These are detailed below.

4.2 Senior Management

The Chief Financial Officer (CFO) and Executive Management shall be responsible for the following activities within the Access Intelligence ISMS:

- Agreeing the business need for this ISMS, and communicating their ongoing commitment to it
- Reviewing and signing off this Information Security Policy
- Setting and reviewing Access Intelligence's Information Security Objectives
- Delegating appropriate resources necessary to manage and operate the ISMS effectively
- Agreeing the level of acceptable risk within the Risk Assessment Methodology (**see ISDL31**)
- Approving any decisions not to address any unacceptable residual risks, where identified

- Having ultimate responsibility for actions related to information security incidents breaches
- Overseeing any disciplinary action resulting from information security incidents/breaches

4.3 Information Security Manager

The Information Security Manager shall have functional responsibility for the Access Intelligence ISMS, and shall be responsible for the daily operational tasks of the ISMS, including:

- Ensuring an appropriate structure of ISMS policies, processes and work instructions
- Ensuring that appropriate records are created and maintained for all ISMS activities
- Ensuring the ISMS operates in accordance with the current requirements of ISO 27001:2013
- Arranging a programme of risk assessments, risk treatments and internal audits
- The preparation and communication of the Statement of Applicability
- The provision of an appropriate user training and awareness programme for employees
- Overall management of the information security controls in production processes
- Overall management and functionality of Access Intelligence's business continuity plan
- The provision of a user training and awareness programme for suppliers and contractors.
- The design and review of technical security controls, including Access Intelligence's networks
- Supporting reviews, internal audits and risk assessments within their area of responsibility

4.4 Department/Function Managers

Managers within Access Intelligence shall be responsible for:

- Ensuring that their team members are aware of and remain compliant with all information security policies, processes and work instructions, and they receive relevant training for their role
- The provision of a user training and awareness programme for applicable third-party users
- Supporting reviews, internal audits and risk assessments within their area of responsibility

4.5 Asset Owners

As per the Asset Management Policy (**ISDL05**), designated Asset Owners shall be responsible for:

- Assessing the value of their asset(s) to the Company
- Undertaking detailed risk assessments on their asset(s), including the identification of controls and assessing their effectiveness (as per the Risk Assessment Methodology **ISDL31**)
- Addressing any unacceptable risks (as per the Risk Assessment methodology **ISDL31**)
- Helping in the investigation, resolution and closure of any information security incident which directly or indirectly affects the security of their asset(s).
- Reviewing and authorising the levels of access to their asset(s) which are granted to others (as per the Access Control Policy **ISDL07**)
- Contributing to the Acceptable Use Policy (**ISDL06**), specifically for the user of their asset(s)

4.6 Control Owners

As per the Asset Management Policy (**ISDL05**), Control Owners shall be responsible for:

- The way in which their assigned control(s) are selected, implemented and operated
- Understanding which asset(s) are reliant upon each of their assigned controls

- Contributing feedback to asset owners on the operation of each control, to assist them in undertaking accurate risk assessments of their asset(s)

- Helping in the investigation, resolution and closure of any information security incident which does or does not indicate the failure of a control.

All individuals specified within the scope of this Information Security 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.

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	David Roud	31/10/2018	First version, to enable Access Intelligence to achieve ISO 27001:2013 accreditation
2.0	Ato Abraham	26/11/2019	Change of leadership team, outsourced IT Service Provider has changed to new company, ISO 27001:2013 needs to be renewed, GDPR has replaced Data Protection Act 1998
3.0	Adam Palmer	19/01/2021	ISO 27001:2013 accreditation was achieved in June 2020. Updated roles and responsibilities. Also, included references to ISDL10, ISDL13, ISDL19, ISDL54, ISDL77, ISDL390.
4.0	Adam Palmer	22/11/2021	Updated Senior Management structure. Included references to ISDL03, ISDL11, ISDL16, ISDL30, ISDL53, ISDL54, ISDL325.

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer		21/01/2020
Mark Fautley	Chief Financial Officer		20/01/2021
Mark Fautley	**Chief Financial Officer**		**20/01/2022**