Access Intelligence Information Security Training Policy

1.0 Policy Objectives

- To ensure that Access Intelligence can operate a trusted, established Information Security Management System, it shall provide appropriate training which ensures that all employees and contractors:

    - are aware of Access Intelligence's Information Security Management System and Objectives;
    - are aware of the threats to information security that Access Intelligence faces, and
    - are aware of their personal involvement in minimising information security risks.

2.0 Policy Scope

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

- All users of Access Intelligence's information assets and information systems, whether employees and contractors, who have an authorised account to access those assets.

- The provision of general information security awareness training to everyone included within this Scope, and the provision of more specific training as identified for the fulfilment of specific duties related to the ISMS (for example for Asset Owners)

3.0 Policy Statements

- New employees, and contractors, must be informed of key elements of Information Security Policy, and their associated responsibilities, as part of 1st day induction on joining Access Intelligence.

- New employees, and contractors, shall be required to attend full information security training within 2 weeks of their start date at Access Intelligence.

- Access Intelligence shall provide refresher information security training which is mandatory for all personnel to complete. This shall cover changes in Access Intelligence's approach to information security, changes to relevant information security processes and communication of any new or changing risks that Access Intelligence may be facing.

- Access Intelligence shall provide detailed training to those individuals who have specific roles and responsibilities in delivering Access Intelligence's ISMS. This shall include, for example, Asset Owners, on how to complete effective risk assessments, and Auditors, on how to effectively perform internal audits as part of the ISMS.

- Information security training shall be provided by any suitable means, including physical training, online portal, documentation, videos and others if needed. Records of all training undertaken shall be maintained and reviewed by Executive Management in the monthly ISMS meeting (see **ISDL09**) and referred to HR if necessary.

- Information security training shall address the following, as a minimum:

    - Access Intelligence's Information Security Policy (**ISDL01**) and information classifications as per the Information Classification Guide (**ISDL52**)
    - Access Intelligence's Acceptable Use Policy (**ISDL06**) and its requirements, including acceptable use of personal devices.
    - Use of passwords as per the Access Intelligence Password Management Policy (**ISDL03**)
    - Identification and reporting of information security incidents as per the Access Intelligence Information Security Incident Policy (**ISDL04**)
    - How Asset Owners protect their assets as per the Access Intelligence Asset Management Policy (**ISDL05**)
    - Accessing information, systems and facilities as per the Access Intelligence Access Control Policy (**ISDL07**)
    - Data protection under the General Data Protection Regulation (**ISDL13**)

4.0 Responsibilities

- The Information Security Manager shall be responsible for providing a schedule of training, including physical sessions and digital/email communications that align with the Access Intelligence Information Security Policy (**ISDL01**) and emerging best practice in this area.

- The Head of HR shall ensure that all new starters are provided with 1st day Security Briefing as part of the new starter welcome process.

- The Head of HR shall ensure that all attendees of information security related training are recorded as having attended and completed such training. They shall also work together with the Information Security Manager to improve and refine the training schedule based on their own assessment and feedback from staff.

- All staff in scope (See Clause 2.0) must complete all assigned training within 2 weeks.

All individuals specified within the Policy Scope of this Information Security Training 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 accreditation
2.0	Ato Abraham	26/11/2019	Change of leadership team, outsourced IT Service Provider has changed to new company, ISO 27001:2013 certification needs to be renewed
3.0	Adam Palmer	18/01/2021	ISO 27001:2013 certification was renewed in June 2020
4.0	Adam Palmer	10/09/2021	Updated training timeframes

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**