Access Intelligence Asset Management Policy

1.0 Policy Objectives

Access Intelligence shall, as an essential element of its Information Security Management System **(ISMS)** ensure that all its information assets are **always** identified and protected. This extends to those supporting assets upon which information assets depend for their confidentiality, integrity and availability.

All assets shall be subject to risk assessment, and appropriate controls identified and applied to ensure that risks are fully managed. Security controls shall operate both efficiently and effectively in an authorised manner to ensure that Access Intelligence's information and supporting assets are protected.

2.0 Policy Scope

Access Intelligence's Asset Management Policy shall cover:

- All information assets (data) owned by Access Intelligence
- All information assets (data) belonging to a client and entrusted to Access Intelligence under an agreement which specifically details Access Intelligence's responsibility for the security of that data.
- All supporting assets, including premises, hardware, software, information systems, networks (treated as hardware and software) and media, upon which the security of the information assets rely.
- The selection, implementation and effectiveness of controls used to manage risks to both information assets and supporting assets.

3.0 ***Policy Statements***

Asset Management, as required for the Access Intelligence Information Security Management System, shall be undertaken by the delivery of activities by specific individuals, as detailed below:

- The Information Security Manager shall be responsible for:
    - The creation and maintenance of the Inventory of Assets, which shall contain all identified information assets and the supporting assets upon which they rely.
    - Organise a biannual review of the Inventory of Assets with Asset Owners.
    - Liaising with Senior Management and Leadership team to check that all information within Access Intelligence is correctly recorded within the Inventory of Assets, and to make any additions, amendments or deletions as may be required.
    - Undertaking, in conjunction with the Asset Owner, a high-level risk assessment of each information asset to assess the impact of a breach of confidentiality, a breakdown of its integrity or a reduction in its availability. This activity shall be conducted in accordance with the ISMS Implementation Guide (**see ISDL31**) and provides a criticality assessment for each information asset which shall be recorded.
    - Assessing the results of risk assessment and risk treatment activities undertaken by Asset Owners, to (a) ensure that they are accurate and of an appropriate standard, and (b) to identify when additional support or assistance may be required.
- Asset Owners shall also be responsible for:
    - Undertaking regular risk assessments of information and supporting assets that they are responsible for, in accordance with the ISMS Implementation Guide (**see ISDL31**), and for undertaking any risk treatment activities that arise from the identification of unacceptable risks.
    - Regularly reviewing the Access Intelligence information security policies and processes, to ensure that their assigned assets continue to be managed and operated in a manner which complies with them. This exercise shall be undertaken by all Asset Owners, whether their assets require a full risk assessment, or are of a lower sensitivity classification or criticality such that only Baseline Controls have been applied (**see Appendix A of the ISMS Implementation Guide ISDL31**).

- The Security of any assets for which they are responsible that need to be moved off-site for any reason, for example for maintenance or repair. All such assets shall only be relocated once any sensitive or protectively marked information contained on them has been securely and permanently deleted.
- The security of any assets for which they are responsible that need to be moved between Company sites for any reason. All such assets shall only be moved once any sensitive or protectively marked information contained on them has been confirmed as having been subject to the appropriate security controls, e.g. hard disk/solid state drive encryption.
- The security of any assets for which they are responsible that are to be disposed of, or re-purposed. Such assets shall only be disposed of or re-purposed once all information contained on them has been securely and permanently deleted.
- The assessment of the physical security controls which are provided by the premises that house assets for which they are responsible, and for raising any security concerns over levels of physical security with the Information Security Manager.
- Engaging in the investigation, resolution and any corrective actions resulting from information security incidents (**see ISDL04**) which either directly or indirectly indicates gaps in the protection afforded to an asset for which they are responsible.

- Control Owners shall be responsible for:
  - Ensuring they understand which assets their assigned control(s) are helping to protect, and that their control(s) are being properly managed and operated efficiently to afford the maximum protection to these assets.
  - Regularly reviewing the Access Intelligence information security policies and processes, to ensure that the controls that they are responsible for continue to be managed and operated in a manner which complies with them.
  - Engaging in the investigation, resolution, and any corrective actions resulting from information security incidents (**see ISDL04**) which either directly or indirectly indicates gaps in the effectiveness of/or security being provided by one or more controls for which they are responsible.

- Individual employees shall be responsible for:
    - Understanding the value, importance and security of Access Intelligence assets, which shall be communicated by the Access Intelligence Information Security Training Policy (**see ISDL02**)
    - Ensuring that they use Access Intelligence assets strictly in line with the Access Intelligence Acceptable Use Policy (**see ISDL06**) and any other specific documentation which has been issued and relates to the use of specific assets.
    - Reporting any potential or actual security weaknesses that relate to Access Intelligence assets and controls in prompt manner and using the specific communication channels, as detailed within the Access Intelligence Information Security Incident Management Policy (**see ISDL04**)

4.0 Responsibilities

This policy document defines specific activities that shall be performed by:

- Information Security Manager
- All Assigned Asset Owners
- All Control Owners

All individuals specified within the scope of this Asset Management 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	New assets have been acquired from Response Source, ISO 27001:2013 accreditation needs to be achieved.
3.0	Adam Palmer	18/01/2021	ISO 27001:2013 accreditation was renewed in June 2020
4.0	Adam Palmer	15/11/2021	The Inventory of Assets is now updated biannually

Approver(s)

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