Access Intelligence Internal Audit Policy

1.0 *Policy Objectives*

- Access Intelligence operates a rolling programme of internal audits, in order to assess the performance and effectiveness of all the Company's Management Systems by determining whether:
    - Each conforms to the documented requirements of applicable British or International Standards, and any applicable legislation or regulations
    - They continue to align with Access Intelligence goals and objectives
    - They are being properly managed, implemented and maintained
    - Any identified corrective or preventive actions required are implemented

2.0 *Policy Scope*

- Access Intelligence's Information Security Management System (ISMS), and all related activities that are necessary to allow Access Intelligence to continue to conform to the ISO27001 international standard, including all policies, processes, control objectives, controls and records.

3.0 *Policy Statements*

- Access Intelligence shall compile and communicate in advance, a programme of internal audits, which shall include details of audits which have been arranged to cover the activities, functions and processes detailed within the Scope of this Policy
- The frequency of internal audits for each activity, function or process shall be determined by the organisation after full consideration of:
    - The activity's level of criticality to the organisation
    - The documented results of previous internal audits
    - The existence of any known issues, incidents or operational challenges
    - Whether the activity is new and has not been subject to an internal audit before.

- Internal Audits shall be undertaken by suitably qualified, experienced and competent Internal Auditors. Auditors shall not undertake (or be asked or be expected to undertake) audits which include their own work. Auditors shall be expected to prepare, undertake and document internal audits in accordance with current best practice.

- The results of internal audits shall be promptly and accurately documented and presented to the appropriate Manager. Any identified risks or non-conformances should be logged on the InfoSec Risks Register and handled according to our defined Risk Treatment Methodology.

- The appropriate Manager of the activity, function or process shall be required to investigate and resolve any reported non-conformance by implementing permanent corrective and/or preventive actions within the requested timescales. The Internal Auditor shall arrange to return and review these actions before the internal audit can be signed off as completed.

- Internal audit reports, and statistics from them, shall be presented to Executive Management for review as they are available. Internal audits reports shall be formally reviewed as part of the Annual Management Review Meeting, and if needed at a Monthly Management Review, (as per the Management Review Policy, **ISDL09**).

4.0 ***Responsibilities***

- The Information Security Manager shall be responsible for ensuring that a rolling programme of internal audits is conducted, in accordance with the internal audit timetable, by appropriate Internal Auditors. They shall also be responsible for ensuring that internal audits are promptly documented and communicated, that non-conformances are addressed in a timely manner, and that Executive Management are provided with reports and statistics.

- Executive Management shall ensure that appropriate resources are allocated to conduct internal audits that address the Scope of this Policy. They shall review internal audit reports as they are issued, and take any actions deemed necessary in response to the audit findings. They shall formally review the internal audit programme at the Annual Management Review and more often if necessary.

- Department/Function/Process Managers shall attend audit opening and closing meetings with the Auditor and shall ensure that their personnel are available to participate in the audit at the date and time agreed with the Auditor. They shall also be responsible for reviewing and signing off the internal audit report, and for implementing required corrective and/or preventive actions to address any non-conformances which have been identified.

- All personnel shall be required to participate in internal audits as required.

5.0 *Document Version Control*

This policy needs to be reviewed annually as an absolute minimum, or if required changes ae 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	Amendments made to document in readiness for ISO 27001 Stage 1 audit
3.0	Adam Palmer	20/01/2021	ISO 27001 accreditation was achieved in June 2020
4.0	Adam Palmer	13/12/2021	Annual approval

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer		12/03/2020
Mark Fautley	Chief Financial Officer		26/02/2021
Mark Fautley	**Chief Financial Officer**		**20/01/2022**