Access Intelligence Management Review Policy

1.0 *Policy Objectives*

- To ensure that Access Intelligence undertakes regular, formal management reviews of its Management Systems, to validate that they are operating as planned and remain relevant to business activities.
- To ensure that Access Intelligence has defined participants, responsibilities and structure of all formal management reviews, including the format and distribution of documented records.

2.0 *Policy Scope*

Access Intelligence's Management Review Policy shall include the following:

- The Access Intelligence Information Security Management System (ISMS) including policies, processes, work instructions, templates, information security risk assessment and risk treatment records, information security incident records, internal and external audit reports, client specific information security documentation and any other relevant documentation.

3.0 *Policy Statements*

Access Intelligence shall undertake formal reviews of its Information Security Management System as follows:

3.1 Monthly Summary

- This formal meeting shall be to communicate to Executive Management the ongoing activities of the ISMS within Access Intelligence, to escalate any matters requiring Executive Management intervention, and to seek approval for any actions requiring Executive Management approval.

- This meeting shall be attended by the Information Security Manager, at least one Director of the Company, and any other participants required in line with the agenda items.

- This monthly meeting shall have the following regular agenda items:

    - a review of significant risk assessments completed over the previous month
    - a review of any significant risk treatment activities over the previous month

- a review of internal audits and non-conformances raised over the previous month
- a review of ISMS metrics (KPIs and KRIs)

- The monthly meetings will contain the following agenda items at least once per year:

  - a review of risk assessments since the last meeting
  - a review of any risk treatment activities since the last meeting
  - a review of any new or changing threats that need to be addressed by the ISMS
  - a review of internal audits and non-conformances since the last meeting
  - a review of information security incidents (**see ISDL04**) since the last meeting
  - a review of feedback from stakeholders/interested parties since the last meeting
  - a review of progress towards the Company's current information security objectives
  - a review of any recent or planned business changes which may affect ISMS activities
  - a review of the need for any process changes or additional training
  - review of the impact of any legislative, regulatory or contractual changes which may affect the ISMS

- This meeting shall produce the following outputs:

  - Feedback to specific Asset Owners on the content of their asset risk assessments
  - Executive Management approval, as Risk Owner, for all risk treatment activities where residual risks have been identified and remain
  - Documented actions arising from recent internal audit non-conformances and information security incidents, including, as applicable, process changes, control changes and any training plans
  - Documented actions arising from the review of progress towards information security objectives, including any changes needed to ensure their achievement
  - If applicable, specific feedback to stakeholders/interested parties who provided inputs
  - Monthly Risk Report, including activity summaries and metrics

- Minutes of this meeting shall be formally recorded and distributed to attendees and relevant personnel.

3.2 Annual Review

- This formal meeting shall be to communicate to Senior Management the ongoing activities of the ISMS within Access Intelligence over the previous year, and plan for the next period. This meeting shall be the forum for establishing and reviewing information security objectives, key ISMS policies, and certain KPIs and thresholds required for the operation of the ISMS.

- This formal meeting shall be a formal review attended by at least one company director, Executive Management, the Information Security Manager, significant Asset Owners

- This meeting shall have the following agenda items:

    - a review of the risk assessments completed over the previous year
    - agreement on a plan for risk assessments for the forthcoming year
    - a review of any risk treatment activities over the previous year
    - agreement on any residual/accepted risks being carried into the forthcoming year
    - a review of internal audits and non-conformances raised over the previous year
    - agreement on a plan for internal audits for the forthcoming year
    - a review of information security incidents (**see ISDL04**) over the previous year
    - a review of the previous year's information security objectives
    - agreement on the information security objectives for the forthcoming year
    - a review of the Information Security Policy (**see ISDL01**)
    - a review of the ISMS Manual/Implementation Guide (**see ISDL31**)
    - a review of the ongoing suitability of the ISMS to meet the requirements of ISO27001
    - a review of key KPIs and thresholds which trigger actions within the ISMS
    - a review of the effectiveness of security training (**see ISDL02**) over the previous year
    - a review of feedback from stakeholders/interested parties over the previous year
    - agreement on a plan for information security training for the forthcoming year
    - a review of any planned business changes which may affect operation of the ISMS
      consideration of any suggestions for improving the overall operation of the ISMS

- This meeting shall produce the following outputs:

    - Documented risk assessment plan for the forthcoming year
    - Documented residual/accepted risks being carried forward into the forthcoming year

- Documented internal audit plan for the forthcoming year
- Documented information security objectives for the forthcoming year
- Documented information security training plan for the forthcoming year
- Agreement (or agreed changes) to key ISMS documentation
- Agreement (or agreed changes) to current ISMS activities
- Agreement (or agreed changes) to ISMS KPIs and thresholds*
- If applicable, specific feedback to stakeholders/interested parties who provided inputs

- Minutes of this meeting shall be formally recorded and distributed to attendees and relevant personnel.

4.0 ***Responsibilities***

The Information Security Management System (ISMS) will be formally approved by Executive Management.

Governance, Review and Authorisation

- The Board has the overall responsibility to set the risk appetite and to ensure governance and oversight

- The Executive Management team sets internal policies and procedures based on the Board's direction

- The ISMS will be prepared by the Information Security Manager in consultation with Executive Management. It will be reviewed, challenged and authorised by the Board, and reviewed by internal and external auditors

- The ISMS is created and updated based on inputs from the business plan and management discussions.

4.1 Information Security Management System

This Policy shall primarily involve Executive Management and the Information Security Manager. Additionally, Asset Owners, Control Owners and Process Owners shall be required to attend monthly reviews and/or the annual review, should the agenda identify their direct or indirect involvement in activities that are to be discussed.

The Information Security Manager shall be responsible for scheduling Management Review meetings, ensuring that the agenda is covered, outputs agreed, and minutes recorded.

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	Ato Abraham	26/11/2019	First version created for ISO27001:2013 accreditation
2.0	Adam Palmer	19/01/2021	Annual policy approval
3.0	Adam Palmer	15/11/2021	Updated monthly meeting requirements

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**