Access Intelligence Supplier Security Management Policy

1.0 *Policy Objectives*

- Access Intelligence uses third party suppliers to provide services and goods. The effective management of these suppliers is essential in the provision of services to Access Intelligence's clients and ensuring the security of Access Intelligence's systems and data. The Supplier Security Management Policy describes control requirements for Suppliers who manage commercially sensitive or confidential information, including any personal data.

- To ensure protection of the organization's assets that are accessible by suppliers.

- To maintain an agreed level of information security and service delivery in line with supplier agreements.

2.0 *Policy Scope*

Access Intelligence's Supplier Security Management Policy applies to:

- Third party organisations, including but not limited to suppliers, contractors, and consultants, who have responsibility for the management, processing, storage or deletion of Access Intelligence information assets, or responsibility for information processing facilities upon which information assets rely for their security.

- Access Intelligence staff involved in supplier management.

- Commercially sensitive or confidential information, including but not limited to, personal data.

Access Intelligence's Supplier Security Management Policy includes:

- Requirements which must be adhered to when engaging any third party which has access to any information assets or information which belongs to, or is the responsibility of, Access Intelligence.

- Standard terms that should be included in supplier agreements.

- How Access Intelligence will monitor compliance.

- How changes related to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed.

3.0 *Policy Statements*

3.1 General Statements

- When it is required for Access Intelligence to outsource services to a third party, it shall comply with the requirements detailed in this policy. This may include a variety of types of suppliers, including but not limited to; facilities management, IT suppliers, financial services providers, waste collection, to whom the organization will allow access to its information and facilities.

- The assessment of third-party organisations prior to their formal engagement by Access Intelligence shall include a review of the maturity of their own information security capabilities. Preference will be shown in the selection process to those third parties who have formal certification, including Cyber Essential Plus, ISO 27001:2013 and SOC2. Where formal certification does not exist, suppliers will be required to demonstrate experience in safeguarding information assets and processing facilities by completing a Supplier Security Questionnaire Assessment (SSAQ). Additional contractual clauses may be required depending on the outcome of the security assessment.

- In the case of existing suppliers with access to confidential or commercially sensitive information, assessment should be done retrospectively.

- A risk assessment of supplier activities shall be conducted using the same assessment criteria used in the Inventory of Data Assets (see **ISDL05**, and **ISDL31**). Suppliers with a maximum individual risk assessment (for Confidentiality, Integrity, Availability) of 3 or above will be subject to detailed review as described further below.

- No agreements with a third-party will be approved that increase the overall risk to information security.

- Contractual terms with third party suppliers shall specify Access Intelligence's requirements for Information Security, and Data Protection.

- Access Intelligence shall inform third party suppliers of any relevant requirements related to Statutory, Regulatory and Contractual Compliance that are relevant to

their supply of goods and services. These are defined in: 'ISDL390 Access Intelligence ISMS Statutory Regulatory and Contractual Compliance Policy'

- Access Intelligence and its third-party suppliers shall agree the protective markings, classifications and acceptable use of data, systems, networks and facilities that are to be entrusted either in whole or in part to the third party. The third party shall fully comply with such requirements and shall ensure that its personnel understand their responsibilities in this regard.

- Third party suppliers shall ensure that all dealings with Access Intelligence remain strictly private and confidential and are not disclosed without the prior written permission of Access Intelligence.

- The ongoing information security capability of contracted third-party organisations shall be periodically re-assessed by Access Intelligence to ensure that no risks have been introduced. This shall be included in the asset risk assessment and treatment activities described in the Asset Management Policy (**see ISDL05**)

- In some cases, third parties having access to Access Intelligence data assets or facilities will be required to comply with Access Intelligence Information Security Policies which will be supplemented by awareness training of Access Intelligence Information Security Policies and procedures, in-line with 'ISDL02 Access Intelligence ISMS Information Security Training Policy', and will be provided with access to the associated policy documents.

3.2 Event Notifications

- Third party suppliers shall be required to maintain regular communications with Access Intelligence whilst they fulfil the contracted requirements for the delivery of goods and services, and shall be required to promptly notify Access Intelligence of any of the following activities:
    - Any identified security breaches within their own organisation
    - Any actual or potential reasons for ceasing trading, including insolvency
    - Any changes to the status of their information security accreditations, including removal of certification
    - Any changes to directors, key personnel, ownership or operating locations
    - Any formal requests for a government investigation or information disclosure
    - Any proposed change of sub-contractors or sub-processors used in the delivery of providing Access Intelligence with the contracted service

3.3 Audit and Inspection Clause

- The third-party supplier shall unreservedly agree to on-site inspections and audits undertaken by Access Intelligence to ascertain that Access Intelligence information, assets and systems are being properly protected. Where feasible reasonable notice of such an inspection or audit shall be given, and any attempts by the third party to avoid or unreasonably delay such activities shall be reviewed by Access Intelligence which may lead to the termination of the services.

3.4 End of Service Requirements

At the end of the contract for delivering goods or services to Access Intelligence:

- Access Intelligence shall arrange to promptly revoke access to all premises, facilities and systems to which the third-party supplier had been granted access

- The third-party supplier shall fully adhere to Access Intelligence's requirements for returning all Access Intelligence information assets, including providing evidence of the secure and permanent erasure of Access Intelligence data from the third-party supplier's systems and backup media.

- The third-party supplier shall be obliged to notify all its personnel of the ongoing requirement to confidentiality and the obligations of the non-disclosure agreement.

3.5 Risk Assessment and Treatment

Any information security issues, or deficiencies identified by Access Intelligence with respect to the products or services provided by a third-party organisation shall be reported to the Information Security Manager and recorded as an Information Security Incident (**see ISDL04**)

4.0 ***Responsibilities***

- Access Intelligence's Information Security Manager shall be responsible for ensuring that this Supplier Security Management Policy remains current, aligned with Access Intelligence business activities and security objectives, and is fully communicated to and understood by those third-party suppliers detailed within the scope of this policy.

- The Access Intelligence Legal Team shall be responsible for ensuring that the requirements of this policy, enhanced by definitive clauses relating to the provision of goods or services by the supplier, are included within contractual documentation.

- Procurement managers must include the Access Intelligence Legal Team and Information Security Manager in the review, negotiation and execution of all contractual documentation regarding new suppliers of company information.

- The third-party supplier shall make their employees and personnel aware of the requirements of this policy and ensure their full compliance with it. Access Intelligence reserves the right to suspend or end the services of the third-party supplier in the event of a proven failure to follow the requirements of this policy in full.

All individuals specified within the scope of this Supplier Security 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 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	Andy Olliver	28/02/2020	Amendments made to reflect changes in business operations post acquisition, ready for Stage 1 ISO 27001 audit
3.0	Adam Palmer	20/01/2021	ISO 27001 certification was achieved in June 2020
4.0	Adam Palmer	15/11/2021	Formalised third-party security assessment requirements

Approver(s)

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