	ISDL No:	ISDL325	Version:	3.0	Class:	Open
	Title:	Access Intelligence ISMS Scope				

Access Intelligence ISMS Scope

1.0 Purpose

The purpose of this document is to precisely define assets, locations, technology, etc. that are part of the scope.

The purpose of the Access Intelligence ISMS is to:

- Ensure that Access Intelligence understands and manages security-related risks to assets and services it manages
- Provide leadership, direction and visible management support for information security
- Provide a framework for the reporting and review of information security incidents
- Provide a central resource of all security related information for all Access Intelligence employees and contractors
- Demonstrate compliance with the principles and practices of ISO 27001:2013 to staff, auditors and clients.

2.0 Context of the Organization

Access Intelligence is a tech innovator, delivering high quality SaaS products that address the fundamental business needs of clients in the PR, marketing and communication industries.


The portfolio includes Vuelio, the platform that helps organisations make their stories matter; ResponseSource, a network that connects media and influencers to the resources they need, fast; and Pulsar, an audience insights and social listening platform.

Access Intelligence is listed on AIM and our technology is used by more than 3,500 global organisations every day, from blue-chip enterprises and communications agencies to public sector organisations and not-for-profits.

An integral component of each of the business units within the portfolio is the development, hosting, support, and maintenance of software and systems for processing group and client data.

In September 2021, the Access Intelligence portfolio was strengthened with the acquisition of Isentia, a leading media intelligence platform in APAC. For clarity, as integration will take some time, when "Access Intelligence" is mentioned in the ISMS Information Security Policies, it will exclude Isentia.

This document must not be copied, loaned or used without prior written consent of AI. If this document is printed, confirm current version via SharePoint prior to use.	Version No:	3.0	Page 1 of 4
---	-------------	-----	-------------

	ISDL No:	ISDL325	Version:	3.0	Class:	Open
	Title:	Access Intelligence ISMS Scope				

3.0 Needs and expectations of interested parties

Interested parties include clients, investors, staff, regulatory bodies.

Requirements of interested parties relevant to information security:

- Clients (UK and International):
 - Secure management of data about client, and client users.
 - Provision of SaaS tools with appropriate protection from cyber-security risks.
 - Secure storage and processing of client data using methods that protect it's confidentiality, integrity and availability.
 - Accurate contract and billing management.
- Investors:
 - Management of corporate risk related to cyber-security concerns. i.e. do not create risk to overall company value or reputation through becoming victim to cybersecurity incidents.
- Staff:
 - Protection of staff data related to employment and salary.
- Suppliers:
 - Access is reviewed regularly
 - Formal agreements regarding information security
- Regulatory Bodies, and Law:
 - Ref ISDL390 Access Intelligence Statutory, Regulatory and Contractual Requirements Policy for list of relevant regulations.
 - The Information Commissioners Office. This is the independent regulatory office (national data protection authority) dealing with the Data Protection Act 2018 and General Data Protection Regulation, the Privacy and Electronic Communications (EC Directive) Regulations 2003 across the UK; and the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 in England, Wales and Northern Ireland and, to a limited extent, in Scotland.


4.0 Scope of ISMS

The ISMS encompasses all activities within Access Intelligence's portfolio of businesses, which includes: Vuelio, ResponseSource, Pulsar. Until further notice, the ISMS scope does not include Isentia.

The scope includes business activities relating to:

- The provision of development, operation, maintenance and support of Internet and Web services and systems.
- Employment of staff.

This document must not be copied, loaned or used without prior written consent of AI. If this document is printed, confirm current version via SharePoint prior to use.	Version No:	3.0	Page 2 of 4
---	-------------	-----	-------------

	ISDL No:	ISDL325	Version:	3.0	Class:	Open
	Title:	Access Intelligence ISMS Scope				

- Managing supplier relationships.
- Managing client relationships.
- Managing investor relationships.

The Scope Statement to be used for ISO 27001 accreditation is:

'The design, development, management and provision of public relations and public affairs, marketing intelligence and communications software as a service solutions, based in the UK.'


5.0 Document Version Control

This document 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 scope of Access Intelligence's ISMS.
- 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 document, together with its previous versions, shall be recorded below.



This document must not be copied, loaned or used without prior written consent of AI. If this document is printed, confirm current version via SharePoint prior to use.	Version No:	3.0	Page 3 of 4
---	--------------------	------------	-------------

	ISDL No:	ISDL325	Version:	3.0	Class:	Open
	Title:	Access Intelligence ISMS Scope				

Version History

Revision	Author	Date	Reason for issue
1.0	Andy Olliver	02/03/2020	Creation
2.0	Adam Palmer	20/01/2021	Annual policy review
3.0	Adam Palmer	15/09/2021	Adjust scope of ISMS to exclude Isentia. Added expectations of suppliers.

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer		20/01/2021
Mark Fautley	Chief Financial Officer		17/09/2021