Access Intelligence Information Classification and Handling Policy

1.0 *Policy Objectives*

- To ensure that all information processed within Access Intelligence is classified and handled according to the standards described in this Policy, and that all employees and contractors:

    - are aware of Access Intelligence's Information Classifications
    - are aware of the principles of data access for each classification
    - are aware of their personal responsibilities for classifying and handling information.

2.0 *Policy Scope*

Access Intelligence's Information Classification and Handling Policy shall include the following:

- All users of Access Intelligence's information assets and information systems e.g. Office 365, whether employees and contractors, who have an authorised account to access those assets.
- 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.
- Commercially sensitive or confidential information, including but not limited to, personal data.

3.0 *Policy Statements*

- All users with access to Access Intelligence business information (see Section 2.0) are responsible for considering the most appropriate Information Classification (see Clause 4.0) for the data.
- All users must apply Information Classification labels to all information assets e.g. suppliers, documents, emails.
- If Information Classification labels cannot be applied to a document, e.g. Google Workspaces, for any information to be classified 'Confidential' or above, all users should manually add the classification label to the top of the document.
- When electronically sharing/transferring information, classified as 'Sensitive' or above:

- from within a cloud environment e.g. in Google Workspaces or Office 365, users must select the option which would provide the most protection.
- via email e.g. attaching a spreadsheet to an email, users must consider appropriate security controls in relation to the sensitivity and criticality of the information e.g. password protect the attachment, encrypt the email.

- When physically transferring business information, e.g. carrying a laptop, physically moving files, information assets must not be left unsecured and unattended.
- On receiving information with a classification label, recipients must respect the handling guidelines (see Clause 6.0) and process the data accordingly.

4.0 *Information Classifications*

4.1 Open

Information marked as **OPEN** should have no serious or detrimental effect on an organisation in the event of its unauthorised or accidental disclosure or its loss. Information classified as Open can be shared externally and viewed openly and publicly.

Examples of information which may be classified as OPEN include press releases, white papers and research documents, certain policies and processes, and any other information that could be openly shared with all employees, clients and competitors.

Information within this category is unlikely to require encryption, due to its nature, and is therefore will not be subject to the Company's Encryption Policy.

4.2 Sensitive

Information marked as **SENSITIVE** should be restricted to personnel within the organisation itself, and trusted external individuals or organisations. Typically, the external elements should be under a contractual obligation (i.e.: Confidentiality or Non-Disclosure Agreement (NDA)) to protect this information type and understand how it is to be protected.

Examples of information that may be classified as SENSITIVE include service reports, performance data, client/supplier contractual agreements, and any other information that should not be shared with the entire client base or a competitor.

Information within this category may require encryption, dependent on the information in Section 6.0 below, and therefore may be subject to the Company's Encryption Policy (**see ISDL11**).

4.3 Confidential

Information marked as **CONFIDENTIAL** should be restricted to personnel within the organisation only, and this information type should never be disclosed externally. Personnel are free to share this information internally with other members of the workforce.

Examples of information that may be classified as **CONFIDENTIAL** include financial budgets and reports, company strategies and plans, details of forthcoming changes to products and services, and any other information that should not be shared with clients, suppliers or anyone else outside of the organisation.
Information within this category will require encryption, as detailed with Section 6.0 below, and therefore will be subject to the Company's Encryption Policy (**see ISDL11**).

4.4 Secret

Information marked as **SECRET** should be restricted to certain personnel or identified groups within the organisation: due to its sensitivity, this information type should not be disclosed to the entire workforce.

Examples of information that may be classified as SECRET include remuneration, payroll and benefits details, and any other information that should not be "common knowledge" amongst the workforce.

Information within this category will require encryption, as detailed with Section 6.0 below, and therefore will be subject to the Company's Encryption Policy (**see ISDL11**).

5.0 ***Principles of Data Access***

One of the most significant principles of Information Security is that access should only be provided to those who have a legitimate and justified need to access that information. Even if an individual holds an appropriate security clearance, that on its own does not give them automatic access to information of a corresponding classification: the information asset owner needs to grant and remove access based upon validated requirements.

Within an organisation, it is common practice for new employees to have only the most basic access to information and IT facilities, which can then be modified based upon their progression or increased responsibilities in their career. Care needs to be exercised when an employee changes position or department to review their access rights and adjust accordingly. Employees who leave the company should have all their access rights revoked immediately.

Further information is given in the Access Control Policy **(ISDL07)**.

6.0 *Information Handling*

	Open	Sensitive	Confidential	Secret
Labelling of Digital Docs	No restrictions. Sensitivity Labelling in Office365 labels documents and emails 'OPEN' by default.	Ensure Sensitivity Labelling for Documents and Emails is updated to appropriate classification.		
Labelling of Printed Docs	No restrictions.	Mandatory, at the top of the page. Added automatically by Office 365.		
Photocopying	No restrictions	With care, collect promptly		
Sending by Post or Courier	No restrictions	Single envelope, marked with recipient's details	Signed for service only. Double envelope, inner one marked appropriately.	Signed for service only. Double envelope, inner one marked. Check for signs of tampering.
Transmitting by Internal Email	No restrictions	No Additional requirement above Sensitivity Labelling of Email, and associated attachments.		
Transmitting by External Email	No restrictions	NDA for external: consider encryption	NDA for external: preference for encryption	NDA for external: compulsory encryption
Access on Mobile Devices in Public Places	Care to avoid possible eavesdropping	Not recommended, avoid if possible	Prohibited	
Information when Travelling (e.g. on laptops, memory sticks etc.)	Care should be taken	Ensure data is encrypted when stored. e.g. laptop full disk encryption.		
Printing of Information	No restrictions	With care, collect promptly	With care, and only to printer in immediate vicinity	
Storage of Info in Printed Form	No restrictions	Dependent upon specific content	Locked drawer, filing cabinet or safe	
Disposal of Info in Printed Form	Recycling	Shredding, or secure disposal	Shredding, or secure disposal	
Disposal of electronic information (digital file).	Removal of file-system entry for file.		Use desktop file shredding tool to ensure secure deletion of file system content.	
Disposal of physical medium (e.g. hard disks/drives).	Information must be disposed of securely using state of the art approved solutions for the permanent removal of data. A record must be kept of how, when and by whom the information was destroyed (to provide an audit trail).			
Reporting Loss, Theft or Compromise	Not required	Raise an Information Security Incident		

7.0 Responsibilities

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

- The Access Intelligence IT Team shall be responsible for ensuring that the Information Classifications specified in this Policy are available in all systems where information is regularly shared. If it is possible to add technological controls to these classifications, then these options should be discussed with the Information Security Manager.

- All staff and contractors should be aware that Human Error is the main cause of Data Leaks. Individuals are responsible for considering the sensitivity of the information that they are processing and correctly classifying the document i.e., choosing the appropriate "Sensitivity Label" in spreadsheets and emails.

All individuals specified within the scope of this Information Classification and Handling 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.

8.0 Document Version Control

This guide 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 guide, 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 guide, 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	31/01/2020	Changes made to align with updated encryption policy, and also text amended in Section 3.0.
3.0	Adam Palmer	20/01/2021	ISO 27001 certification was achieved in June 2020
4.0	Adam Palmer	13/08/2021	Upgraded Guide to Policy by adding objectives, scope, statements and responsibilities.

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer		31/01/2020
Mark Fautley	Chief Financial Officer		20/01/2021
Mark Fautley	**Chief Financial Officer**		**20/01/2022**