Access Intelligence Access Control Policy

1.0 Policy Objectives

All information assets, and their supporting assets, shall be afforded such protection as is necessary to ensure that their confidentiality, integrity and availability can be maintained to required levels. This shall include the selection and implementation of suitable controls to prevent loss or damage by unauthorised access, unauthorised amendment, and deliberate and accidental damage.

2.0 Policy Scope

Access Intelligence's Access Control Policy shall include the following:

- All information assets, either owned by Access Intelligence or entrusted to Access Intelligence by a client under an agreement which specifically details Access Intelligence's responsibility for that data, and including:
    - Information assets held, processed or stored on Access Intelligence premises, and
    - Information assets held, processed or stored at approved off-site premises.

- All supporting assets (for example premises, IT systems and networks) upon which the security of information assets depend.

- This policy shall apply to all Access Intelligence employees, whether full-time, part-time, permanent, temporary or casual. It shall also apply to any contractors or third-party users who have authorised access to any Access Intelligence information assets.

3.0 Policy Statements

3.1 General Access Control Policy Statements

- Access Intelligence shall operate all access control activities upon the principle of "least privilege" and specific permission is needed to enable specific access to be provided, in accordance with the individual's role and bona-fide business needs.

- The level of protection and access to an information asset shall be in line with:

    - The business needs for the individual to access the asset
    - The security classification of the asset
    - The security of the environment in which the information asset is to be accessed
    - The security clearance and competencies of the persons requiring access
    - The requirements of the Access Intelligence Acceptable Use Policy (**see ISDL06**)

- Access Intelligence shall manage user access to information assets (including SaaS suppliers) via the following JML processes:

    - **Joiner** – An access request form is completed by the hiring manager and submitted to Office Management. Only access to assets for the new starter's role will be granted. The Office Manager organises access for the new starter with Asset Owners and IT Support.
    - **Mover** - An access request form is completed by the hiring manager and submitted to Office Management. Only access to assets for the new starter's role will be granted, any previous redundant access must be terminated. The Office Manager organises access changes for the user with Asset Owners and IT Support.
    - **Leaver** – HR to notify Office Management of a user's last day. The Office Manager notifies Asset Owners and IT Support to terminate access at the end of the last day.

- Each Asset Owner (as stated within the Information Security Policy: **ISDL01**) shall be responsible for reviewing, authorising and recording the details of those persons who have legitimate access to their asset(s).

- Whilst every attempt is made to keep access current, all access permissions shall be reviewed every six months (as a minimum) to ensure that they remain accurate and current, and adjusted as necessary. Asset Owners must document this activity with the Information Security Manager for audit requirements.

- All access controls shall be configured and managed to record both successful and unsuccessful access events. Access control records shall be reviewed on a regular basis, and any suspicious activities logged as an Information Security Incident (**see ISDL04**) for immediate investigation.

- If available, Two Factor Authentication (2FA) must be enabled for each asset.

- Any VPN (Virtual Private Network) must have 2FA enabled for all external access.

- Electronic or biometric physical access controls must be in place at all physical locations under the control of Access Intelligence.

- Any secure areas protecting information assets must have appropriate environmental controls which alert asset owners to a significant change in environmental conditions.

- Access to removable media must be disabled on all Access Intelligence owned assets.

- All access and privileges shall be fully revoked immediately at the point at which an employee leaves the employment of the organisation or changes their role within the organisation. A similar obligation shall be placed upon the organisations responsible for contractors or third-party users.

3.2 Acceptable Use of Computers and Information Systems

- All users accessing information assets electronically shall have a unique User ID assigned by Access Intelligence, which shall be used to access only those information assets for which the user has been specifically authorised and has a genuine and on-going business need.

- Users shall not use generic User ID details to access information assets, nor shall they use super user accounts, e.g. supervisor or administrator privileges, unless such privileged account access is essential under the prevailing circumstances.

- Users shall ensure that their User ID is supported by personal passwords which fully comply with the Access Intelligence Password Management Policy (**see ISDL03)**

- When accessing Access Intelligence information assets, all users shall comply with the Acceptable Use Policy (**see ISDL06**)

3.3 Access to Premises

- All Access Intelligence premises shall be protected by appropriate access control mechanisms, so that the identity of personnel is verified prior to them being granted access to the building. This shall include the issue of entry fobs and/or physical keys.

- Any user who fails a security check (either automated or when challenged) shall be denied access to the premises.

- An Information Security Incident (**see ISDL04**) should be raised for investigation in the case of unauthorised or unidentified visitors.

- Lost fobs and keys should be logged as an Information Security Incident (**see ISDL04**) by the designated owner, so they can be blocked, and potential unauthorised access prevented.

- At the point of termination of a permanent employee or contractor, all access fobs and physical keys shall be recovered by the Head of HR and/or Office Manager, and the individual immediately removed from all appropriate access lists. The Office Manager shall periodically review authorised access to the premises, and immediately remove any permanent employee or contractor who no longer needs to access to the asset in question from a business perspective.

- Visitors to Access Intelligence premises shall be recorded within the Visitors Book and shall be issued with a distinctive visitor's lanyard/badge, available from the building's reception, that they shall always be required to wear. The visitor's badge shall be visibly distinct so that they can be immediately identified as being a visitor. Visitors shall always be escorted whilst on Access Intelligence premises and shall surrender their visitor's lanyard/badge when leaving.

3.4 Remote Access Policy by Internal Users

- Access Intelligence allows remote access to its systems by authenticated and authorised users, with a valid need for system access. With the use of cloud-based systems, and rise in home-working, the number of systems available for remote access is steadily increasing.

- Access Intelligence shall ensure that all network connections to IT systems and information assets are always protected from unauthorised access, whilst simultaneously allowing and recording the legitimate connections of authorised external users. A request for access shall be reviewed by the Asset Owner (see Section 3.1) and records of access that has been granted shall be kept and maintained.

- All internal users shall receive appropriate communications and formal training to support the approved method of connecting.

3.5 Remote Access Policy by External Users

- Access Intelligence shall ensure that all network connections to IT systems and information assets are always protected from unauthorised access, whilst simultaneously permitting and recording the legitimate connections of authorised internal users. A request for access shall be reviewed periodically by the asset owner (see Section 3.1) and records of access that has been granted shall be kept and maintained.

- All external users shall receive appropriate communications and formal training to support the approved method of connecting remotely.

- All external user connections for which a valid business case has been authorised shall be controlled by an Access Intelligence firewall, router or equivalent network security device. Access shall be logged.

- All end-user devices used for remote access shall be protected by anti-virus software (as detailed within the Acceptable Use Policy: **ISDL06**): such software should be of equal standard to that currently authorised for use by Access Intelligence (currently ESET Endpoint Protection) or if not shall be subject to review and acceptance by Access Intelligence prior to the external connection being authorised.

3.6 Termination of Remote Access Connectivity

- At the point of termination of a permanent employee, contractor or third-party user, all remote access in place shall immediately be revoked by the Information Security Manager or by our outsourced IT Service provider, ITbuilder. The Information Security Manager shall regularly review authorised access to the asset, and immediately remove any internal user who no longer has a valid business need to access the asset concerned.

- At the point of contract termination with an external organisation (including clients, contractors and suppliers), all remote access in place shall immediately be disabled by the Information Security Manager and/or ITbuilder. ITbuilder shall regularly review authorised access to the asset, and immediately remove any external user who no longer has a valid business need to access the asset concerned.

4.0 Responsibilities

- The respective Asset Owner shall be responsible reviewing, authorising (or otherwise) and managing all access to their asset(s). They shall be responsible for undertaking frequent reviews to ensure that all access permissions remain valid for genuine business reasons

- The Information Security Manager shall progress any information security incidents arising from access control breaches or failures.

All individuals specified within the scope of this Access Control 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	Ato Abraham	26/11/2019	Change of leadership team, outsourced IT Service Provider has changed to new company, ISO 27001:2013 certification needs to be renewed
3.0	Adam Palmer	18/01/2021	ISO 27001:2013 certification was renewed in June 2020. 2FA must be enabled if available.
4.0	Adam Palmer	15/11/2021	Formalised JML / staff access management processes

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**