Access Intelligence Acceptable Use Policy (AUP)

1.0 Policy Objectives

- For Access Intelligence's data, information assets and information systems to be protected, an Acceptable Use Policy is actively in place to protect both the individual end user and Access Intelligence. It specifies how systems and infrastructure are to be accessed and utilised in an approved manner, which aligns with the morals, ethics and professional standards of Access Intelligence.

- This Acceptable Use Policy document is designed to ensure that individual end users are notified of acceptable and unacceptable behaviour so that they do not expose either Access Intelligence or themselves to risks or consequential actions or liabilities, either knowingly or accidentally.

2.0 Policy Scope

- Access Intelligence Acceptable Use Policy shall apply to and include all employees, contractors, and third-party users of Company data and information assets, information systems and other resources provided by Access Intelligence for conduction its business activities.
- This Acceptable Use Policy shall apply to all Access Intelligence cloud and physical infrastructure, including but not limited to hardware assets (including servers, desktop computers, laptop computers, and smartphones), software assets (including operating systems and application software), storage assets and use of the network infrastructure.

3.0 Policy Statements

3.1 General Statements

- Information systems and other Access Intelligence resources are provided primarily for authorised company purposes only. Reasonable personal use of company equipment and resources shall be permitted, in conjunction with this Acceptable Use Policy and providing this usage does not access (or attempt to access) any data

and information assets being stored or processed on behalf of Access Intelligence and/or its clients.

- Under no circumstances shall users use information systems to access Access Intelligence information assets other than for their own legitimate business activities. Users shall not access, download, modify, copy, delete, upload or transmit Access Intelligence information other than in strict adherence to published policies and processes which govern legitimate business activities.

- Under no circumstances shall users participate in activities which interfere with the legitimate access or activities of other authorised users or participate in any activity that could result in the denial of access or use of the service to others.

- Under no circumstances shall users be permitted to participate in any activity that is illegal under international or national laws and regulations. Should there be any conflict between such legislation and any part of this Acceptable Use Policy, this shall be escalated to Senior Management as soon as possible for investigation and prompt resolution.

- Acceptable use does not allow users to access, create, process, download, store or communicate any material that is deemed offensive in nature, which, for clarity, includes any words or images that contain:

    - Racial or ethnic commentary or opinions
    - Gender specific commentary or opinions
    - Sexual images, language or suggestive behaviour
    - Excessive or directed profanity
    - Offensive or derogatory comments about one or more persons'
        - ⇒ Age
        - ⇒ Religious Beliefs
        - ⇒ Marital or partnership status
        - ⇒ Sexual orientation
        - ⇒ Disability
        - ⇒ National or ethnic origin
        - ⇒ Political beliefs

- Access Intelligence shall at times comply with requests for information resulting from criminal investigations and legal proceedings, including electronically stored information and data, and therefore reserves the right to enter any of its information systems, and data repositories connected to them, to inspect, review, store or retrieve data within those systems.

- Access Intelligence shall have the right to monitor its employees', contractors and third-party users' access to and use of information assets, information systems, email and voicemail message repositories and other related resources provided by Access Intelligence for conducting its normal business activities. A disclaimer will appear every time an end user logs onto their system after a system restart to remind them of this.

- If this Acceptable Use Policy does not provide enough information on a specific subject, it shall be escalated to Senior Management for consideration and specific approval before activity is permitted to take place.

- Any employee found to have violated any of the requirements of this Acceptable Use Policy shall be subject to disciplinary action, which may escalate up to and include the termination of their employment with Access Intelligence. Any contractor or third-party user found to have violated any of the requirements of this Acceptable Use Policy shall be dealt with as appropriate, including termination of engagement or formal escalation to the contractor's or third-party user's organisation.

3.2 Acceptable Use of Computers and Information Systems

- Users (see section 2.0) shall only work on the laptop provided to them by Access Intelligence. Company laptops contain a variety of security controls pre-configured (**see ISDL30**). Disciplinary action shall be taken against any user found to be attempting to bypass security controls by using a personal laptop.

- Users shall only attempt to access information systems and related resources that they have specific authority to access. Disciplinary action shall be taken against any user found to be attempting to bypass security controls, accessing data not authorised for the user or using another user's account. It shall not be permitted for a user to attempt to "hack" into information systems, data sources or other website either internally or externally, and users shall always comply with the Access Intelligence Access Control Policy **(see ISDL07).**

- All information systems and related resources shall be protected by strong passwords (which comply with the requirements of the Password Management Policy **ISDL03**) and other security controls as documented within the risk assessment for the information system concerned. Information Systems shall be protected by automatic time-out locking after ten minutes of inactivity, or by users locking the system manually (CTRL + ALT + DEL/Windows Key + L) when not being used.

- All information systems and related resources shall be protected by anti-virus software and other software tools installed to protect their normal operations from unauthorised amendment or interference by rogue code. Operating systems and software applications shall be promptly updated with security patches supplied by the vendor, but only once they have been properly evaluated, to ensure vulnerabilities are permanently addressed.

- Anti-Virus software and other protective tools shall be reviewed frequently to ensure that they are providing protection in line with the latest threat and malware lists. Virus definition files must be updated daily.

- Users shall promptly co-operate and comply with instructions issued by Access Intelligence in relation to the upgrading of hardware device firmware and software, where such upgrades have been assessed as being necessary to ensure the ongoing and secure operation of the hardware device and in such cases that require the intervention of the user.

- Access Intelligence information systems and related resources shall not be used to download, process, store, upload or transmit any material that Access Intelligence considers (at its sole discretion) to be obscene, threatening, abusive, offensive to others, defamatory, indecent, racist, sexist, libellous, hateful or connected to criminal or illegal actions or intentions. In addition, acts relating to breaching copyrighted material, trade secrets or violating intellectual property shall also be prohibited.

- Access Intelligence's network infrastructure shall only be used for the purposes for which it has been designed and implemented. Users shall not modify or disrupt any network connectivity or undertake any activity which increases the volume or nature of network traffic to cause disruption to its normal operation. Access Intelligence's network resources shall not be used for transferring non-commercial data other than for "reasonable" use. Access Intelligence consistently monitors and records all network activity.

- All software assets intended to be installed on Access Intelligence information systems shall be submitted to formal Information Security Manager approval, and shall only be authorised if:
    - They have been fully and properly evaluated for information security vulnerabilities
    - They have received specific authorisation from Information Security Manager for the installation

- Access Intelligence holds a valid software license for the intended installation
- They are to be installed strictly in accordance with the vendor's software license
- Access Intelligence has the capability of supporting the software with updates and security patches.

- For clarity, users with local administrator access on their laptop must not install any of the following:
  - Video/TV streaming apps e.g. SkyGo
  - Chat apps e.g. Whatsapp
  - Personal cloud storage e.g. Dropbox
  - Personal VPNs
  - Games

- Access Intelligence reserves the right to monitor and audit instances of installed software on company assets and systems. Any attempts by users to prevent or interfere with such monitoring or audits will be subject to disciplinary action. Users must comply with all requests resulting from security audits within 2 weeks.

- Users (see section 2.0) must not transfer company information to their personal cloud storage accounts.

- The Computer Misuse Act 1990 covers the offences of illegal accessing and using computer systems without authority, and the unauthorised introduction of software into a computer system with the intention of either (a) affecting the normal operation of the computer system, or (b) interfering with any data or program stored or installed on the computer system. Users shall maintain awareness of the offences covered by this law.

3.3 Acceptable Use of Mobile Devices / Bring Your Own Device (BYOD)

- Users of Access Intelligence issued mobile devices, including laptops and smart phones, shall always comply with the issued documented requirements detailing how they are to be accessed, used, stored and protected. Such devices shall be protected by passwords that comply with the requirements of the Password Management Policy (**see ISDL03**). Any actual or suspected loss, theft or misuse shall promptly be reported as an Information Security Incident (**see ISDL04**).

- Mobile devices, including laptops, smart phones and tablets, which are not Access Intelligence assets and have not been issued by Access Intelligence shall not be connected to any information system or network owned by Access

Intelligence apart from the Guest Wi-Fi. The Head Office Wi-Fi network is expressly for the purposes of actions undertaken in pursuit of company aims.

- Users of personal mobile devices, including laptops, smart phones and tablets, which have not been issued by Access Intelligence may install apps from pre-approved suppliers e.g., Office 365. If users are unsure if an app has been pre-approved, they should contact the Information Security Manager. The user must ensure the device is updated with the latest security patches and has biometric authentication enabled.

- Mobile phones connecting to Access Intelligence Office365 system shall be required to enrol with the terms of the configured Mobile Device Management (MDM) and/or Mobile Application Management (MAM) policies.

- Any data that is stored on mobile devices shall be encrypted. If encryption is technically not possible the data storage shall not be permitted. Users of mobile devices shall regularly review the device to purge all unnecessary or historic data. The primary storage medium for a laptop/smart phone user should be OneDrive.

- In the event of an Access Intelligence owned mobile device being lost, stolen or damaged, the registered user shall be liable for part or all the replacement costs, dependent upon the individual circumstances. In the event of multiple or repeat issues, disciplinary action shall be considered.

- The use of mobile phones shall be in accordance with Section 3.6 of this policy and section 4.0 of the Mobile and Personal Device Policy (**see ISDL30**).

3.4 Acceptable Use of Email Systems

- Access Intelligence shall permit reasonable use of Company email facilities for personal use. All such personal use shall be processed, stored and screened as if it were a business communication and shall be made available for inspection as required. The company reserves the right to restrict personal use of email systems at any time.

- Recipients of email messages shall be aware of the consequences and risks of opening emails (and attachments to emails) that may be infected with viruses or other malware. When opening a Word or Excel document that requests for "macros to be enabled", this shall always be answered "no" unless the macro is from a trusted source and the content is expected by the recipient.

- Recipients of email messages shall be aware of the consequences and risks of responding to phishing emails. Before replying to an email, recipients must check the sender name and email address are as expected and that any links target an expected URL. If suspicious, recipients must forward the email to the Information Security Manager.

- Users (see section 2.0) must not transfer company information to their personal email accounts via email.

- Access Intelligence email systems shall not be used for:

    - Commercial ventures not related to Access Intelligence, including the sending of spam or bulk email messages.
    - The transmission or receipt of messages which contain "offensive material", as defined in Section 3.1 of this policy.
    - Sending communications which, by their content or frequency, may be a form of harassment by the message recipient.

- Users of Access Intelligence's email systems for work-related purposes or for posting information to work-related forums or discussion groups shall ensure that:

    - Proper care is taken to address the communication correctly, to minimise the opportunity of the message being undelivered or accidentally misrouted.
    - Unless the intended recipient is committed to a contractual non-disclosure agreement, information being sent shall only be that which is authorised to be in the public domain.
    - Unless the intended recipient is committed to a contractual non-disclosure agreement that covers the intended purpose of the email, information shall not be sent which discloses Access Intelligence locations, operations or employee or client information.
    - Unless specifically authorised by a member of the Leadership Team, any posting or opinions expressed in work related forums or discussion groups shall specifically state that they do not reflect Access Intelligence's position or opinion.
    - They conduct themselves in a professional manner with courtesy, integrity and professionalism, which aligns with Access Intelligence's corporate standing. Users shall ensure that any messages or posts do not violate copyright or intellectual property rights.

3.5 Acceptable Use of Internet and Web Based Groups

- Access to the internet is provided primarily for authorised business purposes and for the conducting of normal Access Intelligence business. Reasonable personal use of this facility shall be permitted. Users shall not access, attempt to access or perform search activities for websites which explicitly contain "offensive material", as defined in Section 3.1 of this Acceptable Use Policy.

- Software (including tools and utilities) shall not be downloaded from the internet to Access Intelligence information systems and associated infrastructure without the prior agreement of the Information Security Manager following the stages outlined in Section 3.2. By default, most users will not have local administrator privileges and therefore will not be able to download software, unless otherwise designated by the Information Security Manager. Users that discover that they can download software freely and without cause should report this to the Information Security Manager or IT Builder for remediation.

- Access Intelligence shall undertake routine monitoring of internet usage by users. Any breach of policies or other abuse of the facility shall be subject to disciplinary action (see Section 3.1)

3.6 Acceptable Use of Telephone Systems

- Access Intelligence's telephony systems are essentially provided for authorised business purposes and for the conducting of normal Access Intelligence business. A reasonable number of personal calls shall be allowed. Users shall keep their personal calls short, making calls to land line destinations where possible instead of mobiles, and shall not make international calls unless for business reasons where no alternative is available.

- Personnel within the Scope of this policy shall not make or receive mobile phone calls from hand-held handsets whilst in control of a motor vehicle. Handsets connected to a hands-free system shall not be used to make outgoing calls unless in an emergency, and incoming calls shall be answered to advise the caller that they should call again later. Access Intelligence accepts no responsibility or liability for fines, penalties and/or driving licence points that are incurred with the use of a mobile phone whilst in control of a motor vehicle.

- Access Intelligence shall undertake routine monitoring of telephone usage by users, including call recording in some cases. Any breach of policies or abuse of telephony facilities shall be subject to disciplinary actions (see Section 3.1)

4.0 Responsibilities

- The Information Security Manager is responsible for organising regular audits to ensure compliance with this Acceptable User Policy is maintained.
- All individuals specified within the scope of this Acceptable User 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. Included new point in 3.4 covering phishing emails.
4.0	Adam Palmer	15/11/2021	Clearer definitions for acceptable personal use of company assets and BYOD

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**