Access Intelligence Mobile and Personal Device Policy

1.0 Policy Objectives

- Ensure Access Intelligence managed mobile devices have effective security controls to appropriately protect access to company data and company systems.
- Ensure personal devices used to access company data or systems do not create unnecessary risk to company data and systems.

2.0 Policy Scope

Access Intelligence Mobile and Personal Device Policy shall include the following:

- Mobile and personal devices, including, but not limited to, computers, laptops, tablets and mobile phones.
- All company managed mobile devices.
- All personal devices used to access company data or systems.
- All staff, contractors, and 3rd parties, who use mobile devices to access Access Intelligence data and information systems.

3.0 Policy Statements

Access Intelligence shall:

- Implement security controls for all company managed laptops including:
  - Full disk encryption
  - Anti-malware – with centralised management and regular rules updates.
  - DNS filtering
  - USB storage blocking
  - Software installation whitelist
  - Minimum privilege for user accounts (**see ISDL07**)
  - Strong authentication (**see ISDL03**)

- Configure company networks, including Ethernet and Wi-Fi, to only allow access to company managed, or otherwise authorised, devices. Non-company devices should only be granted access to company networks with permission of the Information Security Manager.
- Implement Mobile Device Management (MDM) controls to apply appropriate policies to mobile phones and tablets accessing company Office365 accounts. This applies to both personal and company managed devices.

- Implement a Guest Wi-Fi network, with reduced access to company data and systems, to support staff and guest personal devices.

Access Intelligence Staff shall:

- Agree to the terms of MDM enrolment in order to access company Office365 resources through personal and/or mobile devices.
- Not use personal devices to access Access intelligence data or systems, other than for access to Office365 resources. Personal devices should only be granted access to company data and networks, other than Office365, with permission from the Information Security Manager.

4.0 Teleworking

- Access Intelligence supports home working from authorised devices in safe environments. Users must not access business information from a public computer.
- Especially whilst teleworking, staff should remain aware of the Acceptable Use Policy (**see ISDL06 Clause 3.3**)
- Access Intelligence staff must only work on the laptop provided to them by Access Intelligence. Company laptops contain a variety of security controls pre-configured (see section 3.0). Disciplinary action shall be taken against any user found to be attempting to bypass security controls by using a personal laptop.
- Personal smart phones, 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.
- Personal smart phones may only be used when biometric authentication is enabled and the device is still supported with regular security patches. If either is not possible, the user remove all apps with access to Access Intelligence information assets.
- Files downloaded to mobile devices should only be retained for a length of time in which the data is useful and accurate. Device owners are responsible for file retention and should frequently purge local files. OneDrive is the preferred method of storage.

5.0 Responsibilities

Access Intelligence IT Team:

- To implement, and maintain, appropriate end-point controls.
- To implement, and maintain, appropriate network controls.

- To define and manage a client software whitelist and ensure compliance through regular audits.

All Access Intelligence staff, contractors, and 3rd parties:

- To NOT use personal devices to access Access Intelligence data or systems, other than Office365 after successful device enrolment through Office365 MDM controls. Any exceptions to this MUST be agreed with the Information Security Manager.
- To set strong passwords (see ISDL03 Password Management Policy) on any personal device which has access company Office365 resources. If available, biometric authentication is preferred.
- To ensure any personal devices accessing company Office365 resources are updated to the latest versions. If a personal device no longer supports the most recent operating system (e.g. iOS) version, staff must uninstall Office365 and any company files from that device.
- To use company managed cloud storage as much as possible. If there is a requirement to download a company file to a personal device, it must only be retained for as long as required and deleted from the device immediately afterwards.

All individuals specified within the Policy Scope of this Mobile and Personal Device 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.

6.0 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	Andy Olliver	04/03/2020	Inaugural version of this policy, in readiness for ISO 27001 Stage 1 audit
2.0	Adam Palmer	20/01/2021	ISO 27001 accreditation was achieved in June 2020
3.0	Adam Palmer	08/04/2021	Extended staff BYOD responsibilities
4.0	Adam Palmer	15/11/2021	Added teleworking clause

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer		12/03/2020
Mark Fautley	Chief Financial Officer		26/02/2021
Mark Fautley	**Chief Financial Officer**		**20/01/2022**