Access Intelligence Password Management Policy

Passwords are an essential element of information security, providing authentication of users attempting to gain access to information assets and information systems such as networks. The selection of weak passwords, poor password storage or inadequate password management practices could easily lead to the whole organisation being placed at risk. This Password Management Policy provides details on how passwords should be selected and managed within an organisation.

1.0 Policy Objectives

- To ensure that Access Intelligence's information assets and information systems are afforded relevant protection from unauthorised access using effective user identification and password verification. This includes both internal and external (SaaS) systems.

- To ensure that strong user passwords are created, managed and changed frequently.

2.0 Policy Scope

Access Intelligence's Password Management Policy shall include the following:

- All information assets and information systems that store Access Intelligence data and/or data entrusted to Access Intelligence under an agreement that specifies information security requirements.

- All users of Access Intelligence's information assets and information systems, whether permanent employees, contractors, or third-party users, who have an authorised account to access those assets.

3.0 Policy Statements

- Passwords shall be selected to comply with the following complexity requirements:

    - The password shall contain a minimum of:
        - 8 characters or more
        - at least one upper case character
        - at least one lower case character
        - at least one numeric or special character
    - The password shall not contain all or part of the User ID or the user's name.
    - The password shall not be a single word which can be found in a dictionary (English, or a foreign language), be easy to guess, or be the user's personal information (for example, the name of the user's pet/child)

- The password shall not be or contain an Access Intelligence brand name
- Must not be a password that has already been used as one of the last five user passwords.
- Passwords must not be reused on multiple systems
- The password should preferably be a phrase containing unrelated words, symbols and numbers.
- If a system does not comply with the above complexity requirements, it must be reported to the Information Security Manager to be recorded as a risk.
- If an information asset provides Single Sign On (SSO) or Multi/Two Factor Authentication (MFA/2FA) options, they must be enabled.

- Passwords shall be managed as follows:

  - When supported, all users will be forced to change their passwords every 90 days.
  - When supported, 5 incorrect attempts to enter the correct password will result in the account being locked out for 30 minutes.
  - Initial passwords created for new starters shall be temporary and they will be prompted to change their password at the point of first login to their system.
  - Permanent employees or contractors must not disclose their individual passwords to anyone internal or external to the business. If access is required for another individual, a separate account must be created.
  - Passwords that need to be communicated externally, e.g. during user setup, shall be by secure verbal communication or encrypted electronic communications only.
  - Passwords shall always be sent separately from User ID information.
  - Associated User ID information must be the individual's Access Intelligence email address. Accounts which will have access to company information must never be linked to a personal email address e.g. Gmail, Hotmail etc.
  - Users who have super-user accounts shall maintain these separately from their routine user accounts where necessary, each having separate user IDs and passwords assigned. Such privileged accounts shall only be used when necessary and shall not be used for standard access.
  - **All** user passwords shall be kept confidential, and not recorded in any way which could lead to the password being identified by others. Passwords should **never** be physically written down or shared with other employees.
  - Passwords must not be stored in plain text on work machines e.g. Word, OneNote, Email etc.
  - If permanent employees or contractors feel the need to store and/or record multiple passwords for different systems or sites, then it is highly

recommended for a password management safe to be used. KeePass is recommended on Windows laptops and MacPass on Apple laptops. These password managers are installed on all end user machines by default. The master password for a password safe should not be replicated anywhere in their personal or professional lives. For further guidance permanent employees and contractors should consult the Information Security Manager.

- If it is suspected that a password has been compromised, it shall be reported as an Information Security Incident (**see ISDL04**) and changed immediately.
- All employees, contractors and third-party users shall receive appropriate training on effective password management as part of their information security training. This shall include for example, how to select suitable passwords, and safe usage practices such as not selecting the "remember password" option found in numerous web browsers and common software applications.

- Single Sign On (SSO) using Access Intelligence User Directory should be implemented, when supported, for all systems holding data classified as Sensitive or above.

- Multi-factor authentication should be implemented, when supported, for all systems holding data classified as Sensitive or above.

- Access credentials to all systems should be distinct to a single user, and never shared. Shared passwords should be identified and treated as risks.

4.0 *Responsibilities*

- The Information Security Manager shall advance any information security incidents arising from compromised passwords, by ensuring that the passwords are changed by the user and providing training on password management accordingly.

- All employees and contractors must comply with the password requirements detailed in this policy. Any suspected and confirmed password incidents must be reported to the Information Security Manager.

- Asset Owners shall be responsible for ensuring (where possible) all access control systems comply with Access Intelligence minimum standards, for password complexity and management, and where compliance with above standards is not

possible, due to system capability, to treat as a Risk according to defined Risk Management process.

All individuals specified within the Policy Scope of this Password Management 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	01/10/2018	Initial version, to enable Access Intelligence to achieve ISO 27001:2013 accreditation
2.0	David Roud	31/10/2018	Updated sections on LastPass and offline storage

Revision	Author	Date	Reason for issue
3.0	Ato Abraham	26/11/2019	Directory management has changed to JumpCloud and ISO 27001:2013 certification needs to be achieved.
4.0	Adam Palmer	18/01/2021	ISO 27001:2013 certification was renewed in June 2020. Staff changes and re-formatting.
5.0	Adam Palmer	15/11/2021	Additional password complexity and management requirements. Clearer responsibilities for all staff regarding training and incident reporting.

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**