Access Intelligence Data Encryption Policy

1.0 Policy Objectives

- To ensure that Access Intelligence's information assets (data) are protected against breaches or failures of confidentiality, integrity and availability by the appropriate and proper use of encryption, proportionate to the information classification or sensitivity of the data.

- To ensure that only approved cryptographic techniques, software and tools are used by Access Intelligence, and that effective key management and exchange activities are in place.

2.0 Policy Scope

Access Intelligence Data Encryption 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, that:

    - Are owned by Access Intelligence and classified as "Confidential" or "Secret", as defined with Access Intelligence's Information Classification and Handling Guide (see ISDL52), or
    - Are owned by clients, and which carry an appropriate information classification (as confirmed by the client to Access Intelligence) that requires encryption to be in place.

- The hardware and software assets which are responsible for processing or storing the information specified above.

- Networks and associated routing equipment responsible for transit of the information specified above.

- All employees, contractors and third-party users who have a legitimate requirement to access, process, store or transmit information that has a requirement to be encrypted.

3.0 Policy Statements

3.1 Data encryption for secure network transit

- Provided no other restrictions apply, it is permitted for all staff to use computer systems which would normally and by default use encryption, in order to secure data in transit on a communications network.

- Whenever possible and appropriate, encryption shall be used to support security of remote access connections to Access Intelligence's networks and systems e.g. Virtual Private Network (VPN)

3.2 General Encryption Policy Statements

- Access Intelligence shall ensure that all electronic information classified as "Confidential" or "Secret", as defined within Access Intelligence's Information Classification and Handling Guide (ISDL52), shall be encrypted:

    - Where it is stored on a computing device or any computer storage medium which may be exposed to a significant risk of being lost or stolen. Any such device when outside a secure hosting environment is considered to be at significant risk, including laptops and portable devices.
    - Where it is to be transmitted via a computer network using a mechanism that does not itself incorporate encryption. Depending on the specific technology being used this could refer to: sending data by email either within or outside the Company, transferring files offsite, remotely accessing files or Web pages. The risk is that unencrypted data in transit may be intercepted.
    - Where the data is being sent using a postal service such that the data media could be lost, stolen or intercepted and read whilst in transit.

- Access Intelligence will use only standardised, currently accepted, and extensively reviewed encryption algorithms.

- Cryptography implementations must be kept up to date to avoid emerging weaknesses. Follow NCSC guidance on this.

- Encryption of Access Intelligence information shall be provided only using the authorised technologies or software products specified below:

    - Data in Transit is encrypted using TLS 1.2 (or later) on all Websites and Email Servers
    - Data at Rest is encrypted using 256-bit Advanced Encryption Standard (AES) encryption
    - Secure File Transfer Protocol (SFTP) is used for file transfers to relevant bodies
    - Secure Shell (SSH) for securing connections to remote devices.

- All encryption requirements specified by clients shall be:

    - Incorporated into contractual documentation
    - Subject to clear understanding of the information classification(s) of the information assets that are to be encrypted
    - Encrypted only using the authorised technology or software products specified above: if the client specifies an alternative then this shall be subject to prior evaluation and approval by Access Intelligence.

- All personnel identified as being in the Scope of this Encryption Policy shall maintain their own encryption (and decryption) keys in a private and confidential manner, similar to the way in which they manage passwords. All keys shall be changed frequently.

- Any suspected or actual loss or breach of encryption (or decryption) keys shall be escalated immediately as an Information Security Incident (see ISDL04), and the keys changed. Any external person(s) or organisation(s) party to encrypted information exchanges affected by such an incident shall be informed.

- Access Intelligence reserves the right, subject to a Senior Management written request, to request any key, password or similar used to store information on company-owned hardware assets.

3.3 Management of Encryption Keys

- Procedures must be in place:
    - To manage encryption keys in a way that ensures encrypted stored data will neither become unrecoverable nor accessible by an unauthorised person.

- To facilitate authorised members of Access Intelligence to obtain prompt access to the encrypted information in the case of an emergency or investigation.
- To ensure that encryption keys are stored and always communicated securely.
- To record who holds encryption keys relating to important information.
- To revoke encryption keys when key holders leave.

- Where Access Intelligence information received as email (or other means of transport) has been encrypted for secure transit, and is information which may be needed again later, it should be securely stored in a form which does not rely on ongoing accessibility of the sender's public key.

4.0 Responsibilities

- The respective Information Asset Owner shall be responsible for assigning the appropriate information security classification for each information asset, in accordance with the Information Classification and Handling Guide. They shall be responsible for labelling the information's classification (as applicable) and ensuring that this is communicated to all other persons who may access the information asset. They shall be responsible for ensuring that their information is protected by appropriate cryptographic controls as outlined in this Policy.

- The Information Security Manager shall progress any information security incidents arising as a result of encryption breaches or failures, including lost or compromised encryption or decryption keys.

- All employees, contractors, third party users and external users of company information systems shall comply with the requirements of this Data Encryption Policy at all times. Any incident of sensitive information not being stored, processed or transmitted (as appropriate) in a correctly encrypted format shall result in disciplinary action being taken.

All individuals specified within the Policy Scope of this Data Encryption 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	Tanis Jardin	01/11/2017	Initial Version
2.0	Andy Olliver	02/03/2020	Modernised and updated for ISO 27001:2013.
3.0	Adam Palmer	19/01/2021	Annual policy approval
4.0	Adam Palmer	10/12/2021	Regularly monitor current encryption algorithms

Approver(s)

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