Access Intelligence Clear Desk and Clear Screen Policy

1.0 *Policy Objectives*

- For Access Intelligence's data, information assets and information systems to be protected, a Clear Desk and Clear Screen Policy is actively in place to protect both the individual end user and Access Intelligence. This ensures that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of when a workstation is not in use. A Clear Desk and Clear Screen Policy is an important security and privacy control and is an important component of ISO 27001:2013.

- This Clear Desk and Clear Screen Policy document for computer and printer workstations is designed to improve the security and confidentiality of information of end users and Access Intelligence. This policy will mitigate the risk of unauthorized access, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended in the office or whilst working from home.

2.0 *Policy Scope*

Access Intelligence Clear Desk and Clear Screen 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 Clear Desk Policy is applicable whether work takes place in an office or home environment. It is the responsibility of the Office Manager to ensure that this policy is enforced and to ensure regular clear desk and clear screen audits take place.

3.0 *Policy Statements*

3.1 General Statements

- Keys for accessing drawers, strongboxes, filing cabinets or specific rooms should NOT be left unattended at a desk. These should be locked away in your personal locker.

- Computer workstations must be locked when your desk is unoccupied.

- Confidential, restricted or sensitive information, when printed, should be cleared from printers immediately.

- Passwords must not be left on sticky notes posted on or under a computer, nor may they be left written down and left in an accessible location.

- Whiteboards containing restricted and/or sensitive information should be erased.

- When working in a busy environment or if computer screens are visible from a window, staff must use a Privacy Screen cover. These can be provided by the Office Manager.

3.2 Working In An Office Environment

- Laptops and any sensitive and/or confidential paperwork must be removed from the desk overnight and stored in the personal lockers provided by Access Intelligence.

- Under no circumstances shall users place confidential and/or sensitive information in regular wastepaper bins. Documents containing confidential and/or sensitive information must be placed in the designated confidential waste bins located on the first floor.

- The reception area can be particularly vulnerable to visitors. This area should always be kept as clear as possible. No personally identifiable information should be kept on desks within reach or sight of visitors.

3.3 Working In A Home Environment

- All home working activity must conform to the *Access Intelligence Home Working Policy*. Prior to setting up any home workspace, a request for home working must have been granted by either an individual's line manager or HR.

- When planning a home workspace, a *Home Worker Self-Assessment* form must be completed and returned to the Office Manager. The desk for home working should ideally be in a separate room but at least in a dedicated space in which security and confidentiality can be maintained.

- Only company issued computers should be used to access services and applications from home. The use of company equipment is controlled in the Acceptable Use Policy (**see ISDL06**).

- It is preferred that no sensitive or confidential information is printed whilst working in a home environment. If such actions are required, the home worker must inform

the Information Security Manager. When not in use, the information must be stored in a locked container.

- Under no circumstances shall users place confidential or sensitive information in general household refuge sacks. Printed documents containing confidential or sensitive information must be disposed of with a crosscut paper shredder.

3.4 Non-Conformance

- Regular and ongoing Clear Desk and Clear Screen audits will be undertaken to ensure continued employee compliance with this policy.

- This policy requires the participation and engagement of all staff, whether permanent or contractor, to be successful. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.0 ***Responsibilities***

All individuals specified within the scope of this Clear Desk 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	Ato Abraham	26/11/2019	First version to supplement policies already in place which are mandatory for ISO 27001:2013.
2.0	Adam Palmer	18/01/2021	ISO 27001:2013 accreditation was achieved in June 2020. Expanded guidance on home working to incorporate Covid-19 changes.
3.0	Adam Palmer	21/09/2021	Removable media is disabled. Clear Screen audits and privacy screens.
4.0	Adam Palmer	06/01/2023	Annual policy review

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
Mark Fautley	**Chief Financial Officer**		**19/01/2023**