Access Intelligence Adding Information Security Responsibilities into Job Description

1.0 *Overview*

Controls within ISO27001 mandate that employees, contractors and third-party users should have their information security roles and responsibilities documented in accordance with the organisation's Information Security Policy.

For employees over whom the business has direct management responsibility, this is defined within specific ISMS documentation, as well as within the job specification for each role.

For individuals not directly employed by the organisation, e.g. contractors and third-party users, any information security roles and responsibilities should be addressed within the appropriate contracts or agreements as referred to in the Supplier Security Policy (**see ISDL19**)

2.0 *Job Specifications*

Some personnel will have a significant contribution to make to the successful establishment and operation of their organisation's ISMS, and a summary of these contributors can frequently be found within the organisation's Information Security Policy (see **ISDL01)**.

2.1 ISMS Management Roles

These defined roles and responsibilities shall also be extracted and placed into the approved job specification of the individual concerned. For example, the job descriptions for the Information Security Manager would include:

Management of Access Intelligence's Information Security Management System

- *Ensuring an appropriate structure of ISMS policies, processes and work instructions*
- *Ensuring that appropriate records are created and maintained for all ISMS activities*
- *Ensuring that the ISMS operates in accordance with the requirements of the current published version ISO27001 Information Security Management Standard*
- *Arranging a programme of risk assessments, risk treatments, risk treatments and internal audits*

- *The preparation of the Statement of Applicability*
- *The provision of an end-user training and awareness programme for all employees*

2.2 Asset Owner Roles

There will be a reasonable number of employees within the organisation who are assigned the responsibility of being "Asset Owners", responsible for named assets within the Inventory of Assets, including their secure operation, assessing and addressing risks associated with their asset(s), and for promptly investigating and resolving any information security incidents related to their asset(s). These individuals will have the following (or substantially similar responsibilities) within their job specifications:

2.2.1 Responsibilities of Asset Owners

- This position is responsible for the ownership of one or more information assets and/or supporting assets, as defined within Access Intelligence's ISMS Inventory of Assets
- As an Asset Owner, this position is responsible for the secure management and operation of the assigned assets, as defined within Access Intelligence's Inventory of Assets (see ISDL05)
- As an Asset Owner, this position is responsible for the prompt investigation and resolution of any information security incident affecting the assigned assets.

2.2.2 Responsibilities of Risk Owners

There will be a number of Senior Managers within the organisation who are assigned the responsibility of being "Risk Owners". This is an important role in Risk Management as "Risk Owner's Approval" should be obtained for risk treatment plans and the acceptance of any residual information security risks. Suitable wording should be created and added to the job descriptions of roles that are identified as risk owners, or likely to become risk owners in the future.

2.3 Employee Responsibilities

As well as a contractual clause within each employee's Terms and Conditions of Employment, their individual job specifications will conclude with a general clause relating to their responsibilities and participation in the organisation's ISMS, (e.g. see 2.3.1 below):

2.3.1 Information Security Responsibilities of Employees

- This position is within the defined scope of Access Intelligence's Information Security Management System (ISMS). The post holder is responsible for being at all times compliant with the Access Intelligence Information Security Policy and all other policies, processes and documentation which relates to information security within Access Intelligence. Failure to comply will be recorded as a Security Risk and shall result in disciplinary action being taken.

3.0 *Responsibilities*

The Head of HR shall ensure that:

- Individual job descriptions will conclude with a general clause relating to their responsibilities and participation in the organisation's ISMS (see 2.3.1)
- Individual roles with Asset or Risk ownership will include an extra clause relating to their information security responsibilities in the job description
- Any non-compliance will be processed. Disciplinary action must be consistent with the severity of the incident, as determined by an investigation.

The Information Security Manager shall ensure that:

- Any non-compliance that results in a security incident shall be thouroughly investigated (**see ISDL04**)
- Non-compliance is reported to the Head of HR

4.0 *Document Version Control*

This guide needs to be reviewed annually as an absolute minimum, or if required changes are identified to address one or more of the following:

- An identified shortcoming in the effectiveness of this guide, 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	Amended in readiness for Stage 1 ISO 27001:2013 audit
3.0	Adam Palmer	20/01/2021	ISO 27001:2013 accreditation was achieved in June 2020
4.0	Adam Palmer	15/11/2021	Refined clauses for Risk Owners and Non-Compliance. Added Responsibilities.

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**