Access Intelligence ISMS Roles and Responsibilities

1.0 Purpose

To ensure all information security responsibilities are defined and allocated.

2.0 Security Roles

Various Roles have been mentioned within the Policy Documents Library. In each case specific responsibilities have been defined related to each policy.

The Roles defined are:

- Senior Management
- Information Security Manager
- Privacy Team
- Security Team
- Asset Owner
- Risk Owner
- Internal Auditor
- Employee / Contractor

3.0 Role Descriptions

• *Senior Management*

Support from Senior Management is crucial for successful implementation of the Information Security Management System.

The Senior Management role is assigned to a person or group of persons who manage and control the Organization at its highest level, e.g. CEO, CFO, COO

The persons in this role are responsible for:

- Definition of the Organization's strategy
- Definition of goals and the Scope of the Information Security Management System
- Leadership and involvement regarding the Information Security Management System
- Definition of the Organization's operating strategy in the context of data protection through Policies
- Definition of roles, assignment of responsibilities and rights in the Organization

- Provision of resources and budget approval
- Management and supervision of the Organization's external communication
- Participation in Management Reviews and ISMS improvement

- ***Information Security Manager***

The Information Security Manager role is responsible for coordinating all activities related to information security management in the Organization. In small- and medium-sized organizations, this role may be assigned to a single person; in larger systems, it is advisable to assign a group of users to this role.

The person who takes on this role is primarily responsible for:

- Definition and supervision of the Information Security Management System (ISMS)
- Coordination of all activities related to the ISMS
- Communication of information relating to ISMS in the Organization
- Contacting authorities and groups of interest in the area of ISMS
- Supervision and coordination of the Information Security Management System

The person who is designated for this role should have managerial, communication and technical skills.

- ***Privacy Team***

The Privacy Team is responsible for implementation of the requirements set out in UK GDPR, the UK DPA 2018 and other applicable laws governing privacy and the protection of personal data.

- ***Security Team***

The Security Team / IT Administrator Role is the point of contact and responsible for definition, implementation, and technical maintenance of security devices and technologies that constitute the Organization's ICT networks and resources and the Information Security Management System. In small- and medium-sized organizations this may be assigned to several persons, or to a managed service provider; and in large organizations — to IT departments.

The person(s) in this role is responsible, among other things, for:

- Definition and implementation of technical safety measures in the Organization
- Participation in the risk analysis process in the role of a technical expert
- Maintenance of ICT infrastructure and resources based on the Operational Activity Process
- Supervision of access control rights to the Organization's resources
- Monitoring and maintenance of ICT networks and resources of the Organization
- Management of availability, executive potential, and events
- Responding to threats and security incidents in the Organization
- Support and implementation of components constituting a part of operation continuity plans in the Organization
- Raising awareness of users in technological areas

- ***InfoSec Departmental Representative***

Senior Management will assign an InfoSec representative for each department to assist the Information Security Manager. Each department in the Organisation will have an InfoSec Departmental Representative.

The InfoSec Departmental Representative role is about defining who is responsible for each asset in their department. People in this role have overall responsibility of all assets within their department. By default, they are the Asset Owner for all departmental assets but they may assign other Asset Owners to manage specific assets.

Persons in this role are responsible for making sure that all assets within their department are properly protected and managed.

- ***Asset Owner***

The Asset Owner supports the InfoSec Departmental Representative.

Persons in this role are responsible for making sure that each of allocated asset is properly protected and managed.

- ***Risk Owner***

The Risk Owner is the person or entity with the accountability and authority to manage a risk. This is a person who is both interested in resolving a risk, and positioned highly enough in the organization to do something about it.

- ***Internal Auditor***

The Internal Auditor Role is responsible for performing audits. An audit is a systematic, independent, and documented process of collecting audit evidence and its objective assessment in order to determine whether the audit criteria have been met and to what degree. The Internal Auditor Role is important in terms of the maintenance and optimization of the Information Security Management System. Smaller organizations should consider outsourcing this role to external companies specializing in such activities.

The persons in this role are responsible for:

- Participation in the Audit Management Process
- Preparation and distribution of the Audit Report
- Assessment of Organization's compliance with approved security measures in Statement of Applicability
- Preparation of audit criteria to increase its quality
- Development of technical expert skills in the areas required in the Organization
- Improvement and development of management systems in the Organization

The person in this role should be able to combine the practice of auditing Information Security Management Systems with knowledge on the Organization and its security measures in terms of information security. It can be any suitable member of staff if they have received the required training.

- ***Employee / Contractor***

This role represents an Employee/Contractor in your Organization. The competences and knowledge of persons assigned to this role are critical for meeting the Organization's goals regarding information security and data protection. They should work in accordance with applicable policies, processes, and procedures constituting the Information Security Management System.

The most important policies applicable to this Role include:

- Information Security Policy
- Acceptable Use of Assets Policy
- Access to Network and Network Services Policy
- Password Management Policy

Regarding this role, the Organization should focus on building awareness and competences in the area of information security and data protection for existing and new employees.

4.0 Role Allocations

Senior Management:

- The entire Access Intelligence Senior Leadership Team:
  - Mark Fautley - CFO & Board Representative for Corporate Risk Management
  - Joanna Arnold – (Group) CEO
  - Francesco Dorazio – CEO Pulsar
  - Tom Golding - COO
  - Kate Fraser – Head of HR
  - Louise Mendlesohn
  - Stephan Israel
  - Phill Palmer
  - Rob Messana

Information Security Manager:

- Adam Palmer

Privacy Team:

- Adam Palmer
- Lakhan Shah

Security Team

- For Internal IT: role provided by ItBuilder, under direction of Adam Palmer
- For Infrastructure: role provided by Peter Kyrannis
- For Engineering: role provided by Engineering Teams for each product

Departmental Information Security Representatives

- Department Heads hold overall responsibility, but delegated to Departmental Information Security Representatives
  - Adam Palmer – IT
  - Peter Kyrannis – Infrastructure
  - Kyle Lyndsey - Feeds
  - James West – Engineering
  - Stefan Grinstead – Product (Vuelio and RS)
  - Nirain Patel – Product (Pulsar)
  - Daniel Loman - Political

- Megan Train – Research (Pulsar)
- Kelly Gardiner – Research (Vuelio and RS)
- Matt Ward – HR
- Elliott Joseph - Finance
- Maggie Dorrian – Office Management
- Flavius Cerbu – Marketing
- James Bishop - Support & PS
- Oliver Grant - Sales
- Alex Murr – Account Management (Vuelio and RS)
- Claudia Day – Account Management (Pulsar)
- Beth Hallett – Customer Success (Pulsar)

Risk Owner

- Role fulfilled by Information Security Manager or Departmental Representative.

Internal Auditor

- Role fulfilled by an external provider and Departmental Information Security Representatives.

Employee

- All staff

Contractor / Supplier

- All contractors and suppliers with access to Access Intelligence data or systems.

5.0 Document Version Control

This document 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 document, 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 document, together with its previous versions, shall be recorded below.

Version History

Revision	Author	Date	Reason for issue
1.0	Andy Olliver	16/03/2020	Creation
2.0	Adam Palmer	14/01/2021	Updated org structure, staff changes, re-defined Dept Rep and Asset Owner descriptions
3.0	Adam Palmer	10/08/2021	Staff update

Approver(s)

Name	Role	Signature	Date
Mark Fautley	Chief Financial Officer		20/01/2021
Mark Fautley	**Chief Financial Officer**		**11/08/2021**