Access Group
ISMS and PIMS Security Objectives

ISMS and PIMS Security Objectives
Issue No 1.4
Issue Date: 2025/09/11

Global HQ
The Armstrong Building
10 Oakwood Drive
Loughborough
LE11 3QF

1. Introduction

This document outlines the objectives for implementing and maintaining an Information Security Management System (ISMS) and a Privacy Information Management System (PIMS) in accordance with ISO 27001 and ISO 27701 standards for the Access Group. The objectives are designed to ensure the confidentiality, integrity, availability, and privacy of information within Access.

2. Scope

The scope of this document includes all information assets, processes, and systems within Access Group that are critical to its operations, business continuity, and privacy management.

3. Information Security and Privacy Objectives

The following defines the information security and privacy objectives for the Access Group

3.1 Confidentiality

- Ensure that information is accessible only to those authorised to have access.
- Implement access controls and encryption to protect sensitive data.

3.2 Integrity

- Safeguard the accuracy and completeness of information and processing methods.
- Implement measures to prevent unauthorised modification of data.

3.3 Availability

- Ensure that authorised users have access to information and associated assets when required.
- Implement redundancy and disaster recovery plans to maintain business continuity.

3.4. Privacy

- Protect personal data in accordance with applicable privacy laws and regulations in which Access Group operates.
- Implement measures to ensure the lawful, fair, and transparent processing of personal data.

4. Risk Management Objectives

4.1. Risk Assessment

- Conduct regular risk assessments to identify potential threats and vulnerabilities.
- Evaluate the impact and likelihood of identified risks. (OneTrust will allow us to track and prompt individuals to review their risks)

4.2. Risk Treatment

- Develop and implement risk treatment plans to mitigate identified risks.
- Monitor and review the effectiveness of risk treatment measures. (All tracked via OneTrust on its launch)

5. Compliance Objectives

5.1. Legal and Regulatory Compliance

- Ensure compliance with relevant legal, regulatory, and contractual requirements. (Quarterly review of the Legal and Contractual Register)
- Maintain up-to-date records of compliance obligations and status.

5.2. Internal Policies and Procedures

- Develop and enforce internal policies and procedures to support the ISMS and PIMS. (These are annually reviewed – evidence can be found within the document control)
- Conduct regular audits to ensure adherence to internal policies. (The audit schedule and reporting to the SteerCo every 2 months)

6. Continual Improvement Objectives

6.1. Monitoring and Measurement

- Establish metrics to monitor the performance of ISMS and PIMS. (Please see the Cybersecurity and Data Protection Dashboards)
- Conduct regular reviews and audits to identify areas for improvement. (Fortnightly review of the continuous improvement register and the Asana boards track our improvement program)

6.2. Training and Awareness

- Provide ongoing training and awareness programs for employees and contractors. (The LMS demonstrates that 100% employees and contractors are set mandatory e-learning training for both Cybersecurity and Data Protection)
- Ensure that all staff understand their roles and responsibilities in maintaining information security and privacy. (Policy attestation inc. Acceptable Use and Privacy Policies)

7. Communication Objectives

7.1. Internal Communication

- Ensure effective communication of information security and privacy policies and procedures within the Access Group. (Policy attestation inc. Acceptable Use and Privacy policies)
- Foster a culture of information security and privacy awareness among employees. (Quarterly Comms for both Cybersecurity and / or Data Protection)
- Establish a programme to ensure that controls supporting information security and privacy is considered and included within the onboarding and transition of acquisitions into the Access Group. (Documented Process for M&A for Cybersecurity and Data Protection)

7.2. External Communication

- Communicate information security and privacy requirements to external parties, including suppliers and customers. (OneTrust demonstrates this via messaging external parties. External parties need to adhere to The Supplier Code of Conduct)
- Ensure that external parties understand and comply with the Access Group's information security and privacy policies. (Policies are available on the Customer Success Portal to customers and prospective customers)

8. Incident Management

8.1. Awareness and Reporting Incidents

- Access Group shall train and educate colleagues to recognise and respond to security events and incidents to ensure that incidents are managed efficiently in a manner that considers information security and privacy. (100% of employees and contractors are issued the mandatory trainings)
- We will measure and monitor the number of and types of events and report these to senior management. (This is reported through the SteerCo and Audit & Risk Committee)

9. Conclusion

The objectives outlined in this document are essential for the successful implementation and maintenance of the ISMS and PIMS in Access Group. We will regularly review and update the objectives will ensure they remain relevant and effective in addressing the evolving information security and privacy landscape.

10. Document Owner & Approval

The Head of Cyber GRC and Global DPO are the owners of this document and is responsible for ensuring that it is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff on SharePoint. This document was approved by the CISO.

Change History Record

Issue	Description of Change	Approval	Date of Issue
1.0	First release - ISMS Security Objectives retired Jan 24	DPO	2024/01/15
1.1	Annual Review	DPO	2024/03/01
1.2	Update to include further references to “Privacy”	DPO	2024/04/11
1.3	Update to give more structure to the objectives to align with ISO27001:2022	CISO	2024/11/06
1.4	Time format changed & Objectives updated to include measures	Global DPO/MS/FB	2025/09/10