Information Security Policy

Table of contents

Es wurden keine Einträge für das Inhaltsverzeichnis gefunden.

1. Purpose, scope and target audience of policy

This document defines the organisation's information security policy and thus the overarching objective of the Information Security Management System (ISMS). This document defines the purpose, orientation, principles and general regulations for the ISMS.

The information security policy defined in this document relates to the entire ISMS in accordance to the defined scope of the ISMS.

The users of the document are all employees.

2. Terms of information security

Term	**Meaning**
Confidentiality	The characteristic that information is not made accessible or disclosed to unauthorised persons, facilities or processes
Integrity	The accuracy and completeness of the information
Availability	The characteristic that information can be accessed and used by an authorised body if required
Information security	Maintaining the confidentiality, integrity and availability of information
Information Security Management System (ISMS)	Management procedure that deals with the planning, implementation, maintenance,

	review and improvement of information security

3. Importance of information security

3.1. Business objectives

Airsphere's business objective is to provide the best in class passenger management system for airports and airlines. Our solutions aim to enhance operational efficiency and to improve the experience of passengers when travelling through airports. We are aiming to expand our business in the strategic growing aviation markets such as in India, Middle East, Europe, Asia and US. We will expand our product offering with operational tools such as virtual queuing, lounge access and biometric passenger processing as well as offer solutions to increase airport commercial services around SmartDepart app product.

Our passenger management solution is dealing with sensitive passenger data at our customers. We therefore consider Information Security as extremely important.

3.2. Relevant requirements and interested parties

It is particularly important to us that we fulfil the following requirements:

Legal and regulatory requirements such as GDPR. Technological standards as well as customer-specific requirements from airlines and airports and industry-specific standards from aviation organizations such as IATA and ICAO for the implementation of biometric solutions are also important.

We would like to fulfil the requirements and expectations of the following interested parties primarily with the ISMS:

Airlines, airports, passengers, users, supervisory authorities and business partners.

3.3. Information security

Information security is a high priority in line with our business objectives. The objectives for the ISMS are derived from the organisation's business strategy described in section 3.1 and the relevant requirements and interested parties described in section 3.2.

Information security is central to Airsphere as it ensures the protection of sensitive passenger data, builds customer trust and ensures that our innovative passenger management solutions reliably increase operational efficiency and deliver a first-class travel experience.

3.4. ISMS objectives

The objectives of the information security management system are in particular:

- Fulfilment of all ISO/IEC 27001 requirements, in particular successful (re)certification.
- The introduction and regular implementation of ISMS training and awareness-raising measures to increase the information security skills of all employees
- The organization's overall risk in terms of information security should be at most “medium”.
- Preventing information security incidents.

The objectives of the ISMS are documented and their fulfilment checked in accordance with section 3.5. .

3.5. Planning and reviewing the objectives of the ISMS and their fulfilment

When planning how the objectives of the ISMS should be achieved, the planned measures, resources, responsibilities, time targets and the assessment method for the review must be defined. The points must be documented. The objectives of the ISMS and their fulfilment must be reviewed annually. The person responsible for carrying out the review, analysing the results of the review and preparing a review report for management is Information Security Officer.

3.6. Information security measures

The organisation commits to comply with the information security requirements as defined in the subject-specific information security policies and ISO/IEC 27001. Suitable information security controls are identified, defined and reviewed within the risk management framework in the risk assessment and risk treatment methodology.

The applicable information security measures, their implementation status and any exceptions are documented in the Statement of Applicability (SOA). Responsible for the SOA is the Information Security Officer. The SOA must be filed in accordance with the chapter "Management of records to this document".

4. Responsibilities

The following responsibilities exist within the ISMS:

Job title	**Responsible for**
Information Security Officer	- the correct implementation and maintenance of the ISMS in accordance with the information security guideline and ensuring that sufficient resources are available for this. - coordinating the operation of the ISMS and reporting on its performance. - ensuring that annual reviews of the ISMS and any significant changes are carried out and recorded. - the information security awareness of all employees as well as their education and training on the subject of information security.
CEO	- the oversight of the implementation and maintenance of the ISMS in accordance with the information security guideline and ensuring that sufficient resources are available for this. - the definition of the information that is communicated to interested parties in the context of information security.
Lead Developer	the handling of information security incidents and vulnerabilities.
Asset owner	ensuring the integrity, confidentiality and availability of the assets or information for which the person is responsible.
All employees	the reporting of information security incidents or vulnerabilities.

Management Board	the definition of the information that is communicated to interested parties in the context of information security.

All key responsibilities and recurring tasks in the ISMS are managed and documented by the Task Manager in the Digital Compliance Office (DCO).

5. Policy

Information security is anchored at the highest management level of the organisation. The organisation's management is committed to the ISMS in accordance with the requirements of ISO/IEC 27001 and the requirements of risk management in order to adapt the system to constantly changing business conditions and to ensure that the necessary resources are provided. This should enable all relevant ISMS stakeholders to achieve the information security objectives and continuously improve the ISMS. The management is also responsible for implementing the company policy.

6. Obligations and responsibilities in the area of information security

All employees and relevant third parties must be familiar with the organisation's information security policy and the ISMS. All employees must act in accordance with the information security policy, the topic-specific information security policies and all requirements specified by the management. If company policies are violated, disciplinary action may be taken. The management is responsible for communicating the information security policy and emphasising the importance of the ISMS and the company-wide commitment to information security.

7. Referenced documents

The following documents are referenced:

- Scope of the Information Security Management System
- Procedure for Identifying Requirements
- Procedure for Information Security Objectives & KPIs
- Procedure for Corrective Actions

8. Management of records to this document

The following records are kept for this document:

- Overview of ISMS objectives & KPIs
- Report ISMS & KPI target achievement
- Overview of Legal, Statutory, Regulatory, Contractual and other Requirements
- Statement of Applicability (SOA) / VDA ISA catalogue

The records must be kept in accordance with the procedure for the control of documents and records.

9. Document control

This document is valid from 01/01/2025.

The owner of this document is the Information Security Officer, who must review the document at least once a year and update it if necessary.

At least the following criteria must be taken into account when evaluating the document for effectiveness, appropriateness and possible need for adjustment:

- Results of internal and external audits
- Results of the KPI evaluation
- Results of the management reviews
- Adjustments resulting from risk management or corrective actions