PURPOSE AND GOALS

The purpose of the Data Security Policy is to ensure the continuation of *SPEED AIR*'s operations and the minimisation of business losses. This is achieved through the prevention and minimisation of repercussions relating to security incidents.

The Management and all employees commit to comply with Data Security Policies and Procedures according to contextually relevant business goals and the regulatory requirements in effect at any given time.

For this purpose, *SPEED AIR*:

- Develops and enforces policies and procedures that seek to ensure the protection of the organization's information from all potential internal and external threats.
- Commits to comply with operational and legal requirements, as well as standard security obligations.
- Guarantees the reliability, integrity and availability of data.
- Possesses security systems that preclude non-authorised access.
- Creates strategies for the detection and re-evaluation of the risks and repercussions related to potential data security breaches.
- Establishes systems for the recognition, evaluation and handling of threats to the security of information.
- Frequently re-examines the strategic framework it employs to manage threats.
- Inspires client trust by acting in accordance with established security protocols.
- Commits to the continuous improvement of Data Security Systems through establishing and frequently re-assessing quantifiable security goals.
- Devises and implements plans for the restoration and continuation of its operations.
- Communicates all relevant security policies to its employees, partners and other interested parties, depending on the situation.
- Maximises staff compliance with the established data protection procedures by providing training courses and other relevant material.

This policy is enforced in conjunction with *SPEED AIR*'s other policies and procedures.

Policy Scope Statement

This policy pertains to all data and data source users, including:

- The employees of the company,
- Employees of short-term recruitment agencies that work at *SPEED AIR*,
- Business partners and designated staff,
- SPEED AIR's partners or third parties, including suppliers and data processing system suppliers that possess or use information or/and facilities that belong to *SPEED AIR*.

This policy covers all Data Systems that belong to the company or those provided by the company for use by third parties.
The scope of this policy includes all sites, facilities and any other area where SPEED AIR might be present.

Categories of assets: The policy scope applies to all following categories of tangible and intangible assets:

- Equipment
- Software
- Data
- Data processing services
- Human Resources

Further details relating to data assets, systems or resources are documented in the respective inventory file.

COMMITMENT TO DATA PROTECTION

The Management of *SPEED AIR* commits to the constant provision of support and guidance to ensure abidance by security requirements across all levels of the organization.

The Management of *SPEED AIR* has established a robust Data Protection Framework for the development, review and maintenance of data protection procedures in accordance with its business goals.

The Management of *SPEED AIR* commits to the frequent re-examination of its Security Policy in order to ensure that business goals and other requirements are met, that the policy is effective, and that it has been communicated to all employees, as well as any interested external parties.

The Management and staff of *SPEED AIR* are required to comply with Security Policies and Procedures. All users must read, understand and follow this and other relevant data protection policies and procedures. Additional information or clarifications can be provided by line managers or the Data Security Manager.

DATA PROTECTION STRATEGY

Data Security is the protection of information from losses resulting from breaches of confidentiality, integrity or availability. It should not constitute or be regarded as a preventative or restricting factor when conducting business, but as a mechanism that allows for the safe sharing of information.

Data Security protects information from a spectrum of threats, ensuring the smooth running of the organisation, minimising potential business losses, and maximising the benefits from investments and other business opportunities.

The aim of *SPEED AIR*'s Data Security Policy is to make certain of the following:

- Data is protected from any unauthorized access and users are subject to a duty of confidentiality,
- Data integrity is maintained through its protection from non-authorised modifications,
- Data availability to authorised users is guaranteed if and when it is required,
- Regulatory, legal and other requirements are adhered to,
- the achievement of business goals is facilitated.

All of *SPEED AIR*'s employees and involved third parties must abide by this data security policy, as well as other pertinent support policies and procedures. These policies are based on optimal security practices.

ROLES AND RESPONSIBILITIES

All users with access to the company's Data Resource are responsible for the effective protection of the information. The allocation of specific roles and duties is necessary for the protection of data and the proper implementation of the security system.

The primary roles and duties relating to data security are defined and documented as part of the overall description of the company's positions, approved by the Management.

The Management ensures that all necessary human resources are available, and that their skills remain effective through the provision of relevant support (e.g. training, equipment etc.).

POLICIES AND PROCEDURES

Data protection is achieved through the implementation of practices based on established company policies and procedures. The latter can be categorised as follows:

- ***Data Protection Management***
  Aims at providing guidance and support regarding data protection in accordance with business requirements and the relevant rules and regulations. Determines the manner in which policies are written and reviewed.
- ***Data Protection Organisation***
  Aims at creating a systematic framework through which the implementation and efficiency of data protection procedures within an organization can be monitored. Determines and regulates the assignment of duties and procedures that are related to security, as well as matters such as communication with the Authorities and other external entities.
- ***Mobile devices, privately owned devices and Tele-work***
  Aims at ensuring the safety of tele-working and the secure use of mobile devices.
- ***Human Resource Security***
  Aims at ensuring that employees and other contractors have the capacity to carry out their roles and that they understand and fulfil their duties in data protection. Involves security checks before, during and after employment.
- ***Asset management***
  Aims at determining the assets for storage and processing, including data, as well as assigning responsibilities based on their value and importance.
- ***Access control***
  Aims at restricting access to data and data processing systems, applications and facilities, so as to allow only for authorised access and prevent unauthorised access.
- ***Cryptography***
  Aims at delineating the appropriate control measures relating to the use of cryptography.
- ***Area security***
  Aims at defining areas and their limits, as well as safe zones and appropriate access controls, in order to ensure protection from threats, equipment security, safe exit, a clear desk and a clear screen etc.
- ***Operations management***
  Aims at devising operation procedure safeguards, protecting from malicious software and data loss, keeping records, surveilling, identifying and preventing weak spots, performing equipment and system assessments etc.
- ***Communications***
  Aims at protecting data security in networks, ensuring the secure transfer of data and the safe dissemination of information through emails.
- ***Acquisition, Development and Maintenance of Information Systems***
  Aims at ensuring that the acquisition, development and trial of data processing systems are invariably carried out in a manner that guarantees data security.

- ***Relationships with Suppliers***
  Determines the safeguards that need to be included in contracts and the manner in which suppliers are to be monitored.
- ***Handling of Data Security Incidents***
  Aims at ensuring the effective handling and evaluation of data security incidents, devising an appropriate response, collecting evidence, communicating the relevant facts and learning from them.
- ***Operation Continuity Management***
  Aims at guaranteeing the availability of information and the existence of appropriate methods for their processing, even after incidents or events have rendered company facilities practically inoperable.
- ***Compliance***
  Aims at determining effective safeguards regarding the implementation of laws and regulations, protecting intellectual property and the private information of natural persons.

The Management of *SPEED AIR* stands by the totality of its Data Security Policies and Procedures, making sure that they are communicated, understood, implemented and maintained across all levels of the organisation, as well as frequently re-examined in order to remain effective.