Information Security Policy

Itínere Group Management recognises and is aware of the importance of identifying and protecting its information assets, avoiding their destruction, disclosure, modification or unauthorized use. It undertakes to lead and promote security at all levels pursuant to its Security Policy and the targets defined and approved herein, both in general and in particular terms. It will create a Security Management System Information System (ISMS), articulated for compliance with legal and regulatory requirements, to manage protection of the organisation's assets, which will be distributed and published on the corporate website to enable all employees and other interested parties to better understand it.

Information Security is characterised as the preservation of the information's:

a) confidentiality, ensuring that only those with due authorisation can access the information;
b) integrity, ensuring that the information and its processing methods are accurate and comprehensive;
c) availability, ensuring that authorised users can access the information and its associated assets when required.

Information security is achieved by implementing an appropriate set of controls, such as policies, practices, procedures, organisational structures, and software functions. These controls have been established to ensure compliance with the company's specific security targets.

Itínere Group policy is:

- To establish its targets for Information Security on a yearly basis.
- To develop a risk analysis process and, in view of its results, to implement such actions as may be needed to tackle risks deemed unacceptable pursuant to the criteria established in the Integrated Management Manual.
- To establish control targets and their corresponding checks and controls, by virtue of requirements arising from analysis of the risks under management.
- To comply with business, legal and regulatory requirements and contractual obligations relating to security.

- To provide information security awareness and training to all staff.
- To establish necessary means to ensure the company's business continuity.
- To take disciplinary measures should any ISMS policy or procedure be breached.

Itínere Group's Information Security Management Committee undertakes to ensure all staff understand and participate in achieving the ISMS targets.

Every employee is responsible for recording and reporting security breaches, whether confirmed or suspected.

Every employee is responsible for preserving the confidentiality, integrity and availability of information assets pursuant to this policy and the policies and procedures inherent to the Information Security Management System.

Work systems have been established to implement this Itínere Group policy, documented in procedures, instructions, documents and templates that are available to all Group staff. Compliance with these is mandatory for all, including external suppliers of goods and services to the Itínere Group.

Finally, the Itínere Group Management undertakes to continuously enhance the information security management system through security targets; analysis of the security indicators defined for monitoring and measuring ISMS performance; monitoring of the security governance activities and ISMS performance of the Committee; risk management, audit programmes and processing of observations, opportunities for improvement and non-conformities detected by them; analysis of the causes of non-conformities and establishment of corrective actions; analysis of incidents and possible security incidents; management of vulnerabilities, and regular security awareness programmes for all workers.