Information Security Policy

Caravelo (CVO) is a travel tech company that provides subscription solutions to the travel industry. Caravelo helps its clients increase revenue & Market share, improve crisis resilience, and create a better customer experience. Caravelo proprietary platforms directly integrate with existing legacy systems to boost their capabilities and deliver on these promises.

The CVO Management has approved and authorized an information security policy, which is characterised here as the preservation of:

- **Confidentiality** - ensuring that information is accessible only to those authorised to have access.
- **Integrity** - safeguarding the accuracy and completeness of information and processing methods.
- **Availability** - ensuring that authorised users have access to information and associated assets when required.

CVO is committed to preserving the confidentiality, integrity and availability of all its physical and electronic information systems, records and personal data in order to provide assurance that the organization manages information risks.

- So that the needs of service users and platform clients, and the requirements of corporate governance are met;
- To establish confidence that partnership arrangements involving sharing and exchange of information are legal and secure;
- To establish that designed and implemented security features are effective and correct;
- To provide confidence that services and products offered by third party suppliers of information security assurance are adequate and fit for purpose;

Information security requirements will continue to be aligned with CVO goals and the Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations, remote and distributed working and for reducing information-related risks to acceptable levels.

As part of the protection measures, CVO encourages and facilitates information security training to employees as a key procedure to generate awareness and ultimately ensure that any personal information managed by the company is protected from misuse, corruption, loss or unauthorized access.

Control objectives for information security are contained in the ISMS and are supported as appropriate by specific documented policies and procedures. In particular, it is the Policy of CARAVELO to ensure that:

- Information is being managed securely and in a consistent and professional way.

- Information is protected against unauthorized access.
- CVO provides a secure and trusted environment for the management of information used in delivering its business.
- Data protection and confidentiality of information is assured.
- Clear lines of report and supervision for compliance with data protection exist.
- Regular checks to monitor and assess new processing of personal data are carried out.
- Integrity of information is maintained.
- Regulatory and legislative requirements relevant to information systems are met.
- Business Continuity Plans are produced, maintained and tested.
- CVO's information assets are protected through safeguarding its confidentiality, integrity and availability.
- Effective governance arrangements are established, including accountability and responsibility for information security within the company.
- CVO is able to continue and/or rapidly recover its business operations in the event of a detrimental information security incident.
- All breaches of Information Security, actual or suspected, will be investigated and reported to the Chief Information Security Manager.

All employees are expected to comply with this policy and with the ISMS that implements this policy as appropriate to their work roles. All staff, and certain external parties, will receive appropriate training.

This will ensure that information and vital services are available in a usable form to users when and where they need them. It is a key principle of this policy that all information assets (as defined by the ISMS) should have a nominated "owner".

For the purposes of the ISMS assets are defined as

- Critical business applications, filing systems and the information held thereon
- Facilities, networks systems and software under development.

A current version of this document is available to all staff and contractors on the corporate wiki and in the website to external parties. The Information Security Policy will be reviewed annually to ensure its continued improvement.

Date Monday, 17-04-2023

ChangeYourFlight S.L.

DocuSigned by:

Ignacio Uriz Millan

0B8EE2FB049945D...

By, Ignacio Úriz Millán
CEO