INFORMATION SECURITY POLICY

Volaris reaffirms its commitment to the protection, integrity, confidentiality, and availability of information in all its forms, recognizing it as an essential asset for operations and for maintaining the trust of our customers, Ambassadors, and third parties.

Therefore, Volaris is committed to maintaining and continually improving its Information Security Management System (ISMS) through the definition of policies, the implementation of controls, procedures, and technologies aligned with best international practices and applicable regulations.

As part of our commitments, we establish the following key points:

1. Continuous Improvement: Maintain and improve the ISMS through periodic reviews, internal and external audits, and the implementation of corrective and improvement actions on security controls. The results of these activities shall be reviewed by senior management and the corresponding governance bodies.

2. Data Protection and Integrity: Protect data at rest and in transit through appropriate security controls, including encryption when applicable, least-privilege access controls, monitoring, and activity logging. Volaris will implement an information classification model that defines how information must be stored, shared, and securely disposed of to ensure its integrity.

3. Personal Data Protection and Privacy: Volaris shall comply with applicable personal data protection laws, ensuring mechanisms for the collection, use, retention, transfer, and deletion of personal data in accordance with legal, regulatory, and contractual frameworks, as well as coordination with the Legal and Compliance departments.

4. Monitoring and Response: Operate monitoring, detection, and response capabilities for threats and security incidents, including systematic vulnerability management, centralized log collection, definition of severity levels and response times, as well as forensic analysis and investigation activities when applicable.

5. Individual Responsibility: Establish and communicate clear information security responsibilities for all Ambassadors, suppliers, and third parties with access to Volaris' information assets or technological systems. Non-compliance with these responsibilities may result in disciplinary, administrative, and/or contractual actions in accordance with internal policies and existing agreements.

6. Third-Party Security: Ensure that suppliers, strategic partners, and third parties that process, store, or access Volaris information comply with security requirements equivalent to or greater than those of the organization. This includes pre-contract risk assessments, contractual security requirements, vulnerability management programs, encryption, detection and response service levels, and Volaris' right to request evidence or conduct security audits when necessary.

7. Legal and Regulatory Compliance: Comply with laws, regulations, and contractual obligations applicable to information security, personal data protection, and industry-specific requirements, as well as internal policies and corporate standards.

8. Information Classification and Handling: Volaris shall establish an information classification model defining categories, labeling guidelines, access controls, secure storage, transmission, and proper destruction. All Ambassadors and third parties shall handle information according to their classification level to ensure protection throughout its lifecycle.

9. Information Security Risk Management: Volaris shall identify, assess, treat, and monitor information security risks, ensuring that implemented controls are proportional to the level of exposure and aligned with the organization's risk appetite and tolerance. Risk assessments must be conducted periodically and upon significant changes in processes, technology, or infrastructure.

10. Acceptable Use of Information Assets: Volaris shall define guidelines for the acceptable use of devices, systems, email, internet access, mobile devices, and any technological asset, establishing prohibited actions, expected behaviors, and disciplinary measures for improper use.

All Ambassadors and third parties who have access to Volaris information assets must comply with the security policies and procedures, assuming individual responsibility for protecting the systems and information under their management or use. Likewise, the organization establishes specific information security requirements for third parties, suppliers, and strategic partners, ensuring that they maintain the same levels of protection and compliance required by Volaris to guarantee confidentiality, integrity, and availability of shared information.

Volaris seeks to ensure integrity, availability, and protection of data through constant threat monitoring, early vulnerability detection, and timely and effective incident response.

Additionally, Volaris maintains a security culture focused on continuous improvement, Ambassador awareness, and the prevention of technological and business risks. This contributes to achieving the company's strategic objectives and maintaining stakeholder trust. Therefore, this policy establishes a mandatory annual security awareness program, as well as periodic phishing simulations to measure the maturity level of our Ambassadors.

Mónica B. López
Internal Control Sr. Manager