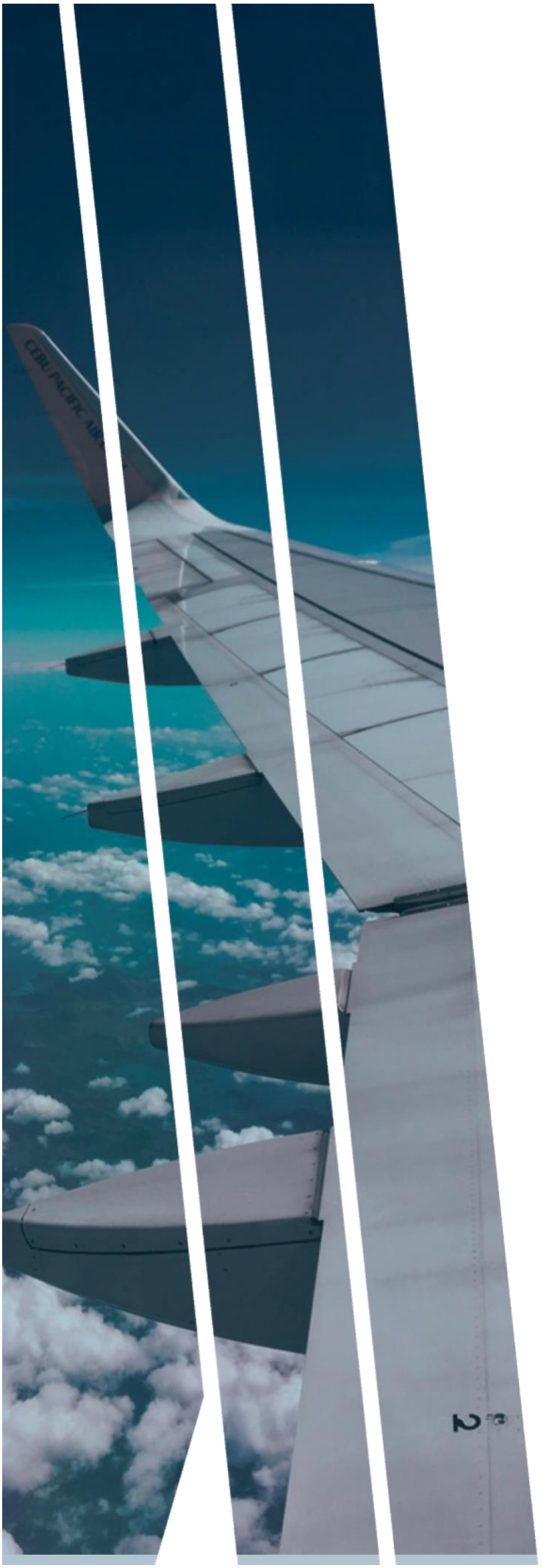


Information Security Policy

DOCUMENT CODE: POL-IT-001

Revision number	Prepared by	Approved by
00	ISMS Manager	VB Group Management

360° Solutions
DIGITAL | FLEXIBLE | GLOBAL

Content

Revision Control

Revision	Date	Change description
00	24/11/2025	Initial version. Implementation.
001	29/12/2025	ISO 27001 requirements have been incorporated.

1. Approval and entry into force

This Information Security Policy is effective as of the date of signature and will remain in force until it is replaced by a new policy.

2. Organization's mission

VB GLOBAL GROUP SL is a company specialized in comprehensive travel management and mobility solutions, with a primary focus on the corporate segment. Our team of professionals combines experience, personalized service, and technology to transform the way companies and travelers manage their journeys.

Through our different brands, we offer innovative and sustainable solutions covering corporate travel, tourism services, and experiences tailored to each client's needs.

Our objective is to be the trusted strategic partner that supports companies and travelers by optimizing resources, enhancing the travel experience, and adding value to every project.

To achieve this goal, VB GLOBAL GROUP SL is committed to information security, ensuring proper management of information in accordance with the requirements established in ISO/IEC 27001:2022 and RD 311/2022 (ENS), in order to provide all stakeholders with the highest guarantees regarding the security of the information used.

The objective of information security is to ensure information quality and the continuous delivery of services, acting preventively, monitoring daily activity, and responding swiftly to incidents. In line with Article 8 of the ENS (Prevention, detection, response, and recovery), departments must be prepared to prevent, detect, respond to, and recover from incidents.

Accordingly, VB GLOBAL GROUP SL systems must be managed with due diligence, adopting appropriate measures to protect them against accidental or deliberate damage that may affect the availability, integrity, or confidentiality of the information processed or services provided.

Likewise, ICT systems must be protected against rapidly evolving threats that could negatively impact the confidentiality, integrity, availability, intended use, and value of information and services. To defend against these threats and ensure continuous service delivery, it is essential to have a strategy that adapts to changing environmental conditions. In this regard, departments must apply the minimum security measures required by the ENS, continuously monitor service performance levels, supervise and analyze reported vulnerabilities, and establish incident response procedures.

This policy is mandatory for all personnel and third parties who, in the performance of their duties, have access to the information or systems described herein.

3. Scope

This policy applies to all information systems that support comprehensive corporate and personal travel management services, including business travel management, corporate travel, conferences, incentives, and MICE services, as well as to information processed in any format.

4. Objectives

Based on the above, Management establishes the following information security objectives:

- To provide a framework that increases resilience and enables effective response capabilities
- To ensure rapid and efficient recovery of services in the event of physical disasters or contingencies that could jeopardize business continuity.
- To prevent information security incidents, insofar as this is technically and economically feasible, and to mitigate information security risks arising from our activities.
- To guarantee the confidentiality, integrity, availability, authenticity, and traceability of information.

5. Regulatory framework

One of VB GLOBAL GROUP SL's objectives is to ensure compliance with applicable legal requirements and any other subscribed requirements, including commitments made to clients, as well as their continuous updating:

- The legal and regulatory framework governing the company's activities includes, among others, Royal Decree 311/2022 regulating the National Security Scheme.

- Regulation (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of personal data.

- Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights.

- Royal Decree 1720/2007 of 21 December, approving the Regulation implementing Organic Law 15/1999 of 13 December on the Protection of Personal Data, insofar as it does not conflict with Regulation (EU) 2016/679 and Organic Law 3/2018.

- Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations.

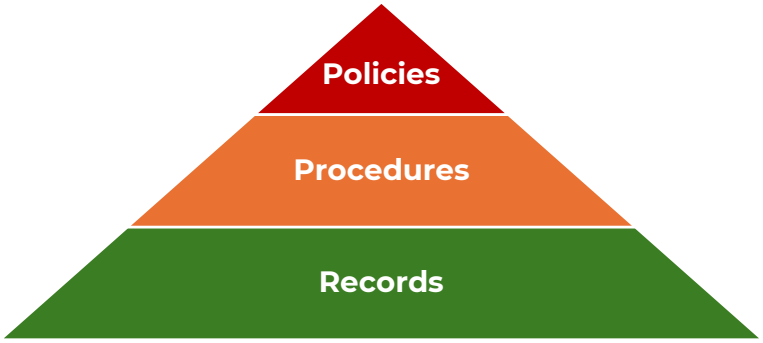
- Law 40/2015 of 1 October on the Legal Regime of the Public Sector.

- Law 34/2002 of 11 July on Information Society Services and Electronic Commerce (ISSEC).
- Royal Legislative Decree 1/1996 of 12 April, on Intellectual Property Law.
- Law 2/2019 of 1 March, amending the consolidated text of the Intellectual Property Law, approved by Royal Legislative Decree 1/1996 of 12 April, and incorporating into Spanish law Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014, and Directive (EU) 2017/1564 of the European Parliament and of the Council of 13 September 2017.
- ISO/IEC 27001:2022 — Information Security Management System framework.

6. Development

To achieve these objectives, VB GLOBAL GROUP SL commits:

- To continuously improving its information security system.
- Identify potential threats, as well as the impact on business operations that such threats could cause if they materialize.
- Preserve the interests of key stakeholders (customers, shareholders, employees, and suppliers), as well as the reputation, brand, and value-creation activities.
- Work collaboratively with suppliers to improve IT service delivery, service continuity, and information security, resulting in greater operational efficiency.
- Assess and ensure the technical competence of personnel, as well as ensure their proper motivation to participate in the continuous improvement of processes, providing appropriate training and internal communication to enable them to implement the best practices defined in the system.
- Ensure the proper condition of facilities and adequate equipment, so that they align with the company's activities, objectives, and goals.
- Ensure a continuous analysis of all relevant processes, establishing the appropriate improvements in each case based on the results obtained and the objectives set.
- Structure the management system in a way that is easy to understand. The management system of VB GLOBAL GROUP SL has the following structure:



The management of the system at VB GLOBAL GROUP SL is entrusted to the IT Systems Manager and will be available in a repository integrated into the company's information system, accessible according to the access profiles granted in accordance with the current access management procedure.

The documentation related to system security is organized in folders within the VB Global Group (All in One) SharePoint environment, divided into subfolders named according to standard points and operational frameworks. These subfolders contain the various procedures, records, and evidence, and access is restricted to company personnel, with no access allowed for unauthorized external personnel.

The security documentation is structured as follows:

- Security Policy.
- Security Regulations: Documents describing the use of equipment, services, and facilities. They define what is considered misuse, personnel responsibilities regarding compliance or violation of the regulations, rights, duties, and disciplinary measures in accordance with current legislation.
- Specific Documents: Security documentation developed according to the applicable CCN-STIC guidelines.
- Security Procedures: Documents detailing how to operate the system elements.

This policy is complemented by the rest of the policies, procedures, and documents in force to implement the entity's management system.

7. Security organization

The primary responsibility lies with the General Management of the organization, which must organize functions and responsibilities, as well as provide the appropriate resources to achieve the objectives of the ENS. Managers are also responsible for setting a good example by adhering to the established security standards.

These principles are embraced by Management, which provides the necessary means and equips employees with sufficient resources to ensure compliance, formalized and made publicly available through this Security Policy.

The defined security roles or functions are:

Role	Duties and Responsibilities
Information Manager (RINFO)	▪ Make decisions regarding the information being processed.
Service Manager (RSER)	▪ Coordinate the implementation of the system. ▪ Continuously improve the system.
Security Manager (RSEG o CISO)	▪ Determine the adequacy of technical measures. ▪ Provide the best technology for the service.
System Manager (RSIS)	▪ Coordinate the implementation of the system. ▪ Continuously improve the system.
Management	▪ Provide the necessary resources for the system. ▪ Lead the system.

This definition of duties and responsibilities is further detailed in the job profiles and in the system documents (Security Committee Minutes).

CONFLICT RESOLUTION
Differences in criteria that could lead to a conflict will be addressed within the Security Committee, and in all cases, the judgment of General Management shall prevail.

8. Security committee

The procedure for their appointment and renewal shall be ratification by the Security Committee.

The committee for the management and coordination of security is the highest authority within the information security management system, such that the most important security-related decisions are agreed upon by this committee.

The members of the Information Security Committee are:

- **SECURITY MANAGER**
- **SYSTEM MANAGER**
- **SERVICE MANAGER**
- **INFORMATION MANAGER**

These members are appointed by the committee, which is the only body authorized to appoint, renew, or remove them.

The Security Committee is an autonomous, executive body with full decision-making authority, whose activities are not subordinate to any other element of the company.

The organization of Information Security is developed in the Security Regulations.

This policy is complemented by the rest of the policies, procedures, and documents in force to implement the entity's management system.

9. Risk management

All systems subject to this Policy must conduct a risk analysis in which the threats and risks to which they are exposed are assessed.

This analysis is reviewed regularly:

- At least once a year;
- When the information being handled changes;
- When the services provided change;
- When a major security incident occurs;
- When serious vulnerabilities are reported.

To standardize risk analyses, the ICT Security Committee will establish a reference assessment for the different types of information handled and the various services provided. The ICT Security Committee will facilitate the availability of resources to address the security needs of different systems, promoting horizontal investments.

The risk analysis will take into account the risk analysis methodology developed in the Risk Analysis procedure.

10. Personnel management

All members of VB GLOBAL GROUP SL are required to be aware of and comply with this Information Security Policy and the Security Regulations, with the ICT Security Committee responsible for providing the necessary means to ensure that the information reaches the relevant parties.

All members of VB GLOBAL GROUP SL will attend an IT security awareness session at least once a year. A continuous awareness program will be established to reach all members of VB GLOBAL GROUP SL, particularly new employees.

Individuals with responsibilities in the use, operation, or administration of ICT systems will receive training on the secure handling of systems to the extent necessary for performing their work. Training is mandatory before assuming any responsibility, both upon initial assignment and in cases of job changes or changes in responsibilities.

11. Professionalism and security of human resources

This policy applies to all personnel of VB GLOBAL GROUP SL and to external personnel performing tasks within the company.

People & Values will include information security responsibilities in employee job descriptions; inform all new employees of their obligations regarding compliance with

the Information Security Policy; manage Confidentiality Agreements with personnel; and coordinate user training related to this Policy.

- Security Management Officer (SMO) is responsible for monitoring, documenting, and analyzing reported security incidents, as well as communicating them to the Information Security Committee and information owners.
- The Information Security Committee is responsible for implementing the necessary means and channels for the Security Management Officer (SMO) to manage system incident and anomaly reports. The Committee will also be informed of incidents, oversee their investigation and progress, and promote their proper resolution.
- The Security Management Officer (SMO) will participate in the preparation of the Confidentiality Agreement to be signed by employees and third parties performing functions at VB GLOBAL GROUP SL, as well as provide guidance on applicable sanctions for non-compliance with this Policy and on handling information security incidents.
- All personnel of VB GLOBAL GROUP SL are responsible for timely reporting of information security weaknesses and incidents they detect.
- Professionalism of Human Resources:
    - Determine the necessary competence of personnel to perform functions affecting Information Security.
    - Ensure that personnel are competent, based on appropriate education, training, or experience.
    - Maintain documented information necessary to demonstrate personnel competence in Information Security.

The objectives of personnel security control are:

- Reduce risks arising from human error, irregularities, misuse of facilities and resources, and unauthorized handling of information.
- Explain information security responsibilities during the employee recruitment stage, include them in agreements to be signed, and verify compliance during the performance of assigned tasks.
- Ensure that users are aware of the threats and risks associated with information security and are properly trained to support compliance with the Information Security Policy in the performance of their regular duties.
- Establish confidentiality agreements with all personnel and users outside information processing facilities.

- Implement the tools and mechanisms necessary to promote the reporting of security weaknesses and existing incidents, in order to minimize their impact and prevent recurrence.

12. Authorization and access control to information systems

Access control to information systems aims to:

- Prevent unauthorized access to information systems, databases, and information services.
- Implement user access security through authentication and authorization techniques.
- Control the security of connections between the VB GLOBAL GROUP SL network and other public or private networks.
- Review critical events and activities carried out by users within the systems.
- Raise awareness of users' responsibility regarding the use of passwords and equipment.
- Ensure the security of information when laptops and personal computers are used for remote work.

13. Protection of facilities

The objectives of this Facilities Protection Policy are as follows:

- To prevent unauthorized access, as well as damage and interference, to the premises, facilities, and information of VB GLOBAL GROUP SL.
- To protect VB GLOBAL GROUP SL's critical information processing equipment by locating it in protected areas, delimited by a defined security perimeter, and equipped with appropriate security measures and access controls. This shall also include protection of the equipment during transportation and when it must remain outside protected areas for maintenance purposes or other reasons.
- To control environmental factors that could adversely affect the proper functioning of the computing equipment that hosts VB GLOBAL GROUP SL's information.
- To implement measures to protect the information handled by personnel in the offices in the normal performance of their routine duties.
- To provide protection proportional to the identified risks.

This Policy applies to all physical resources related to VB GLOBAL GROUP SL's information systems, including facilities, equipment, cabling, files, storage media, and similar assets.

The Security Management Officer (SMO), together with the Information Owners where applicable, shall define the physical and environmental security measures necessary to protect critical assets, based on a risk analysis, and shall oversee their implementation. The RGS shall also verify compliance with physical and environmental security requirements.

The heads of the various departments shall define the levels of physical access for VB GLOBAL GROUP SL personnel to the restricted areas under their responsibility. Information Owners shall formally authorize off-site work involving business-related information for VB GLOBAL GROUP SL employees when deemed appropriate.

All VB GLOBAL GROUP SL personnel are responsible for complying with the clean desk and clear screen policy in order to protect work-related information in daily office activities.

14. Acquisition of products

The various departments shall ensure that ICT security is an integral part of every stage of the system life cycle, from its conception through to its decommissioning, including development or acquisition decisions and operational activities.

Security requirements and funding needs shall be identified and included in the planning process, in requests for proposals, and in the tender specifications for ICT projects.

Furthermore, information security shall be taken into account in the acquisition and maintenance of information systems, by limiting and managing change.

> The information systems development and acquisition policy is set out in the document entitled “Policy on the Acquisition, Development and Maintenance of Information Systems.”

15. Security by default

VB GLOBAL GROUP SL considers it strategic for the organization that its processes integrate information security as part of their life cycle.

Information systems and services shall incorporate security by default from their creation through to their decommissioning, including security considerations in development and/or acquisition decisions and in all operational activities, thereby establishing security as an integral and cross-cutting process.

16. System integrity and updating

VB GLOBAL GROUP SL undertakes to ensure system integrity through a change management process that enables control over the updating of physical and logical components by requiring prior authorization before their installation within the system.

Such assessments shall be carried out primarily by the systems management function, which shall evaluate the impact on system security prior to implementing changes and shall document and control those changes deemed significant or having implications for system security.

Through periodic security reviews, the security status of the systems shall be assessed in relation to manufacturers' specifications, existing vulnerabilities, and applicable updates, and appropriate due diligence shall be exercised to manage risk in light of the resulting security posture.

17. Protection of information at rest and in transit

VB GLOBAL GROUP SL establishes protection measures to ensure the security of information stored or transmitted through insecure environments.

The following shall be considered insecure environments: portable devices, peripheral devices, information storage media, and communications carried out over open networks or networks using weak encryption mechanisms.

18. Personal data

Personal data shall be accessible only to authorized persons. The affected data files and the corresponding responsible parties shall be identified.

All VB GLOBAL GROUP SL information systems shall comply with the security levels required by applicable regulations, in accordance with the nature and purpose of the personal data processed, as set out in the aforementioned Security Document.

19. Third parties

When VB GLOBAL GROUP SL provides services to other entities or handles third-party information, such entities shall be made subject to this Information Security Policy. Appropriate channels shall also be established for reporting and coordination between the respective ICT Security Committees, as well as procedures for responding to security incidents.

When VB GLOBAL GROUP SL uses third-party services or discloses information to such parties, they shall be made subject to this Security Policy and to the Security Regulations applicable to the relevant services or information, and shall be bound by the obligations set forth therein. Third parties may develop their own operational procedures in order to comply with such regulations. Specific procedures shall likewise be established for the reporting and resolution of incidents.

It shall be ensured that third-party personnel are adequately aware of information security matters, at least to the same level as that established under this Policy.

Where any aspect of this Policy cannot be complied with by a third party under the terms set out above, a report shall be required from the Security Officer identifying the risks incurred and the manner in which such risks are to be addressed. Such report

shall be approved by the owners of the affected information and services prior to proceeding.

20. Prevention in interconnected information systems

VB GLOBAL GROUP SL establishes protection measures to ensure Information Security, with particular emphasis on perimeter protection, especially when connections are made to public networks used wholly or mainly for the provision of publicly accessible electronic communications services.

In all cases, the risks arising from the interconnection of the system with other systems through networks shall be analyzed, and the interconnection points of such connections shall be controlled.

21. Activity logs

VB GLOBAL GROUP SL shall record user activities, retaining the information necessary to monitor, analyze, investigate, and document improper or unauthorized activities, thereby enabling the identification of the responsible individual at all times.

The main objectives of Information Security Incident Management are as follows:

- To establish a system for the detection of and response to malicious code.
- To have procedures in place for the management of security incidents and weaknesses identified in the components of the information system.
- To ensure that such procedures include detection mechanisms, classification criteria, analysis and resolution procedures, communication channels with interested parties, and the logging of actions taken.
- Such logs shall be used for the continuous improvement of system security.
- To ensure that IT services return to optimal performance following an incident.
- To reduce potential risks and impacts arising from the incident.
- To preserve the integrity of systems in the event of a security incident.
- To communicate the impact of an incident as soon as it is detected in order to activate alerts and implement an appropriate business communication plan.
- To promote business efficiency.

22. Business continuity

VB GLOBAL GROUP SL, with the objective of ensuring the continuity of its activities, implements measures to ensure that its systems are supported by backup copies and establishes the necessary mechanisms to guarantee the continuity of operations in the event of the loss of customary working resources.

23. Continuous improvement of the security process

VB GLOBAL GROUP SL establishes a process of continuous improvement of information security, applying the criteria and methodology set out in international standards, such as ISO/IEC 27001.

24. Comunication

This Policy shall be communicated to all personnel and shall be made available to the relevant interested parties in the ALL IN ONE document repository.

25. Mandatory compliance

Failure to comply with this Policy may result in disciplinary measures in accordance with applicable legislation.