porvenir
sólo hay uno

Information Security Policy

2025

Business Risk Management

Document's Technical Data Sheet			
Code:	**N-09-SC-RO-SI-03**	**Version:**	5.0
Date of Issue:	November 28, 2018	**Effective Date:**	18 Jun 2025
Process:	Control and Follow-up	**Classification of the information:**	For internal use
Subprocess:	Information Security Risk Management		

Directorate of Organizational Improvement.

CONTENT

1. INTRODUCTION

At Porvenir, information is recognized as one of the most valuable and important assets; it supports the management of internally defined processes. For this reason, it is necessary to have strategies in place that enable effective control and management of information, preserving its confidentiality, integrity, availability, and privacy.

The Company has defined an Information Security and Privacy and Cybersecurity Management System, which includes the Information Security and Privacy and Cybersecurity Policy Manual containing the general policy and specific policies, as a statement of responsibilities and accepted behaviors to maintain the confidentiality, integrity, availability and privacy of the information that is essential for the Company's operation, and the development of capabilities to defend and anticipate cyber threats in order to protect and secure data, infrastructure, systems and applications in cyberspace. It also contemplates the definition of guidelines and directives related to the proper handling of information to effectively manage information security and cybersecurity risks, thus strengthening the culture and awareness of these concepts.

The General Information Security and Privacy and Cybersecurity Policy, defined by Senior Management and approved by the Board of Directors, constitutes the main pillar of the Information Security and Privacy and Cybersecurity Management System, and is taken as the basis for the definition and implementation of controls, security decision-making, information privacy and cybersecurity, and for the development of capabilities to face growing cyber threats.

2. OBJETCTIVE

To achieve adequate levels of integrity, confidentiality, availability and privacy of the Company's information, defining guidelines aimed at regulating the management of information security and cybersecurity within the Company.

3. SCOPE

The General Information Security and Privacy and Cybersecurity Policy, as well as all supporting documents for the Information Security and Privacy and Cybersecurity Management System are a general mandate and apply to:

- All of the Company's processes.
- All levels of the Company, users, customers, third parties (suppliers, contractors), control entities and subsidiaries that internally or externally access information, provide services or have any link with the Company's information

assets.

- All projects associated with the implementation and use of information technologies to operate business processes or to provide the Company's services.
- All information collected, stored, processed, used, preserved or exchanged in the Company's support, regardless of the medium, format, location throughout its life cycle, including distribution, elimination and final disposal, prioritizing its protection according to its classification and under the principles of data life cycle.

4. POLICY

4.1. INFORMATION SECURITY AND CYBERSECURITY POLICY

PORVENIR S.A., a company dedicated to contribute to the growth of its affiliates' savings, supporting them during all stages of their lives, defines its processes and provides its services in a friendly and safe manner, offering high levels of trust during the administration of its clients' resources.

For Porvenir, information is classified as one of the fundamental and strategic assets for the provision of services and efficient decision-making; Therefore, the Company is committed to the proper care and management of its own and its customers' information through the adoption and application of regulatory, normative, and legal frameworks, aligned with international best practices or standards for information security, cybersecurity, and information privacy protection, directing its efforts toward maintaining the confidentiality, integrity, availability, and privacy of its information assets, both on-premise and in the cloud.

The Board of Directors and Senior Management, through the approval of this Policy, declare their position and commitment to comply with the requirements defined in the framework of the Information Security and Cybersecurity Management System, aspects in which the information security and cybersecurity function is directly involved, whose main purpose is to maintain a reasonably secure environment, aligned with Porvenir's mission, strategic objectives and applicable regulatory requirements, defining and implementing good practices to minimize possible impacts derived from an undesired risk that may compromise the essential principles of information security and privacy.

4.2. PERSONAL DATA PROCESSING POLICY

Porvenir, as Data Controller for the processing of personal data, reaffirms its commitment to the protection of our users' data. For this reason, Porvenir's Personal

Data Processing Policy was implemented and is available to our stakeholders in our web site: www.porvenir.com.co. This document is essential because it clearly explains how we collect, use, store and protect the personal information of our stakeholders. It also establishes the rights they have in relation to their data, ensuring that they are informed about how their information is handled and can effectively exercise their rights.

5. COMMITMENT FROM SENIOR MANAGEMENT

Porvenir S.A.'s Senior Management, evidences and strengthens its commitment to the Information Security and Privacy and Cybersecurity Management System as follows:

- Approve the Information Security and Cybersecurity Policy and the Personal Data Processing Policy.
- To provide adequate and necessary resources for the development and implementation of Information Security and Privacy and Cybersecurity initiatives for the operation, thus achieving the maintenance and improvement of the Information Security and Privacy and Cybersecurity Management System, as well as the necessary resources to periodically verify compliance with the obligations and measures adopted for the management of information security and privacy and cybersecurity risks.
- Support management positions in exercising leadership in areas related to the Information Security and Privacy Management System (ISPMS), promoting compliance with ISO/IEC 27001:2022 and ISO/IEC 27701:2020 standards.
- Promote compliance with the policies and standards defined in the Information Security and Privacy Management System.
- Support the creation, conformation and assignment of functions of the Information Security and Cybersecurity Committee, and of the unit that manages information security risks and Cybersecurity.
- Strengthen the management of information security and privacy and cybersecurity risks (loss of confidentiality, availability, privacy and integrity).
- Support the development of cyber resilience competencies and capabilities as well as capabilities oriented to the processing and handling of personal data in the collaborators who manage information security and privacy and cybersecurity risks.
- Promote the culture of information security and privacy and cybersecurity.

- Support the dissemination of policies and other information security, privacy and cybersecurity guidelines.
- Promote information security and privacy management and cybersecurity in projects involving the adoption of new technologies.
- Promote the adoption, application and appropriation of good information security and privacy and cybersecurity practices in order to provide secure products and services in cyberspace that protect data integrity.
- Periodically review the measurement of indicators to determine the effectiveness and efficiency of information security and privacy and cybersecurity management.
- Promote interaction, collaboration and cooperation at the corporate level for the development of preventive measures and response to events or incidents of information security and cybersecurity and/or that have an impact on personal data.
- Establish a communication and information strategy on cybersecurity incidents for reporting to the SFC, competent authorities and financial consumers.
- Collaborate with relevant government bodies and agencies for the improvement of the Company's cybersecurity, compliance with current legislation and contribute to the improvement of cybersecurity at the national level.
- Promote the continuous improvement of the Information Security and Privacy Management System (SGSPI) in accordance with new technologies and methodologies acquired for both information security and privacy.

6. RESPONSIBILITIES OF USERS

Porvenir has structured the functions and responsibilities regarding the Information Security and Privacy Risk and Cybersecurity and their respective management, thus protecting both critical and non-critical information assets for the operation of the business, such as personal data processed by the Entity in accordance with Law 1581 of 2012. The following is the scheme of the three lines, considering:

- Management by line of business,
- An independent Information Security and Privacy and Cybersecurity risk management function; and
- An independent review.

6.1. First Line

The first line is made up of the Information Security - Communications Department and all Porvenir employees. The Information Security and Cybersecurity Policy recognizes the Information Security Management and other collaborators as primarily responsible for identifying, assessing, managing, monitoring and reporting Information Security and Cybersecurity risks and incidents inherent to products, services, activities, processes and safety systems. Those who make up this line of defense must be familiar with its activities and processes, and have sufficient resources to perform their tasks effectively.

Likewise, they must comply with the policies, guidelines and procedures defined by the company, contributing to a solid culture of Information Security and Cybersecurity.

For compliance with the first line on privacy of information, consult the Internal Manual Policies and Procedures Information Privacy Management System.

6.2. Second Line

This line is made up of the Information Security and Cybersecurity Department, which establishes the guidelines in this area and continuously monitors compliance with all Information Security and Cybersecurity risk obligations. The director is responsible for presenting management results directly to Senior Management, the Risk Committee, the Board of Directors or other bodies for consideration. It must have sufficient resources to effectively perform all its functions and play a central and proactive role in the Information Security and Cybersecurity Management System, for this, it must be fully familiar with the policies and standards in force, its

legal requirements and regulations and the Information Security and Cybersecurity risks derived from the business.

For compliance with the second line on privacy of information, consult the Internal Manual Policies and Procedures Information Privacy Management System.

6.3. Third Line

The third line plays an important role in independently assessing the management and controls of Information Security and Cybersecurity risks, as well as the policies, standards, guidelines and procedures of the systems, reporting to the Audit Committee or its designee. The persons in charge of internal audits who are to conduct these reviews must be competent and properly trained and not involved in the development, implementation and operation of the risk/control structure. This review may be performed by audit personnel or by personnel independent of the process or system under review, but may also involve suitably qualified external parties.

For compliance with the third line on privacy of information, consult the Internal Manual Policies and Procedures Information Privacy Management System.

7. APPLICABLE SECURITY AND INFORMATION PRIVACY REQUIREMENTS

Porvenir recognizes the importance of adequately protecting information from threats that could affect business continuity. Therefore, it establishes the development of activities for the protection of information assets, management and administration of Information Security and cybersecurity risks, protection of personal data, security culture, and the behaviors that all Employees and their subsidiaries must adopt. Consequently, all temporary employees and suppliers who, in the course of their activities, use information and technological services at Porvenir and its subsidiaries must ensure: compliance with the requirements and pillars of information security and cybersecurity, protecting the organization's information assets, preserving the confidentiality, integrity, availability, and privacy of information. Therefore, Porvenir and its subsidiaries adopt the following policies on which the Information Security Management System (ISMS) is based and structured. Such Policies are expressions of Senior Management for a fair and transparent presentation and assessment of information security and cybersecurity risks. The above allows for an adequate identification of the controls that reasonably mitigate the risks identified.

7.1. To protect the confidentiality, integrity, availability, privacy and non- repudiation of

information

All Porvenir employees and their subsidiaries must protect and ensure the confidentiality, integrity, availability and privacy of the information, in such a way that the information is not disclosed to third parties:

- Only be accessed by authorized personnel.
- Be concise, precise, with emphasis on accuracy.
- Be available when required.
- Be legitimately accessed and used for what it was authorized for.
- Be treated in accordance with Law 1581 of 2012.

7.2. Adopt and maintain a strong Information Security and Privacy culture Information and Cybersecurity

All three lines must take the lead in establishing a strong information security and privacy and cybersecurity culture where:

- The first line must be an example and replicator of a solid culture and awareness of Information Security and Privacy and Cybersecurity, in compliance with defined organizational policies and procedures.
- The second line must define and implement awareness and culture activities, covering all employees, on the organizational policies and procedures for Information Security and Privacy and Cybersecurity.
- The third line must monitor the execution and compliance of culture and awareness of Information Security and Privacy and Cybersecurity.

7.3. Implement and Maintain a Comprehensive Information Security, Privacy and Cybersecurity Risk Management System

All Porvenir Employees and their subsidiaries shall use a generally accepted internal control framework that defines the elements that are expected to be present and functioning in an effective internal control system. For this purpose, it must be aligned with the corporate methodology of Operational Risk Management - SARO (inherent risk assessment, residual risk and heat map) and with the Corporate Methodologies of Information Security and Privacy and Cybersecurity Risk Management.

7.4. Determine Risk Appetite, Tolerance Level and Risk Capacity

Senior Management, the second line of Porvenir and its subsidiaries shall determine the Risk Appetite, the level of tolerance and the maximum risk capacity, considering

the effect of the nature of its operations and lines of business, as well as the types and levels of information security and privacy and cybersecurity risk that the company is willing to assume at each of these levels. Porvenir's Board of Directors must approve the Risk Appetite, the tolerance level and the maximum risk capacity.

7.5. Establish and maintain a Risk and Opportunity assessment of Information Security and Privacy and Cybersecurity

Porvenir and its subsidiaries must have a process to identify, evaluate, document, manage and mitigate information security, privacy and cybersecurity risks. This process is done at least once a year or when special circumstances occur, identifying risks and assessing their probability and impact, which must be aligned with the corporate methodologies of security risk management and information privacy and cybersecurity.

Likewise, the second line must identify, evaluate and implement both internal and external opportunities that will generate a continuous improvement of the Information Security and Privacy and Cybersecurity Management System.

7.6. Oversee the Administration of the Information Security and Privacy and Cybersecurity Management System

Senior Management and the second line must establish, approve and periodically review the "Information Security and Privacy and Cybersecurity Management System", as well as supervise Management to ensure that policies, processes and systems are effectively implemented at all levels of decision making.

7.7. Establish a continuous improvement process for the Information Security and Privacy and Cybersecurity Management System

The second line should determine the mechanisms for the identification of continuous improvements to the SGSPI that will be implemented according to the value or impact that the application of new technologies or methodologies derived from external best practices will generate for the company.

7.8. Change Management

Senior management and the second line must ensure that there is an approval process that fully assesses information security and privacy and cybersecurity risks

in all new critical processes, activities, products, projects and systems, as well as identifying new threats. For example, every time changes are made to an application that impacts the business, a change committee is held to evaluate the possible risks involved in implementing the change.

7.9. Perform Monitoring and Reporting

Porvenir's second line and its subsidiaries must implement a process to regularly monitor Information Security and Privacy risk profiles and material loss exposures. Additionally, an information security and privacy diagnosis must be performed based on norms, standards and reference frameworks that support information security management and cybersecurity ISO 27000, ISO 27701 and NIST Cybersecurity Framework in order to calculate the level of security and maturity of Porvenir and its subsidiaries by means of Corporate Indicators, Risk Evolution and Control Evolution. Specifically, cybersecurity risks should also be addressed in this regard.

7.10. Control and Mitigate

Porvenir's first and second line and subsidiaries must have a strong "control environment", structured by means of policies, procedures, standards, systems, adequate internal controls and the considered mitigation or compensation of risks. With the above, the first line of defense must have general access controls, privileges, updates in the following minimum aspects:

- Supervision of physical access controls.
- Supervision of logical access controls.
- Monitoring and password protection.
- Supervision and protection of configuration ports and remote access.
- Restriction of application installation by the end user.
- Ensure that operating systems are "patched" with updates or that the controls implemented mitigate the possibility of an incident occurring.
- Ensure that software applications are regularly updated.
- Restriction of administrative privileges (i.e. the ability to install software or change the configuration settings of a computer).
- Ensure that the correct processing of the data is carried out throughout its life cycle, among other compliances associated with the protection of personal data mentioned in the Information Privacy Policy and Standards Manual and in the Personal Data Processing Policy.

7.11. Ensure that the Information Security and Privacy Management System and Cybersecurity Operate in Contingency Situations

The second line or Information Security Leaders of Porvenir and their subsidiaries must ensure that the necessary controls on the pillars of security and privacy of information and cybersecurity are included and implemented in the business continuity plans.

7.12. Ensure compliance with applicable laws and regulations and the requirements of regulatory bodies

It is the obligation of the three lines of Porvenir and its subsidiaries to comply with all the regulations of the regulators in force and the requirements issued by the applicable control entities related to Information Security and Privacy and Cybersecurity.

7.13. Implement Security in New Technologies and Emerging Risks

It is important to implement an information security and cybersecurity plan in relation to new technologies. To monitor, develop and implement remediation strategies for emerging risks, where to:

- Establish security policies on the technologies implemented in Porvenir and its subsidiaries.
- Adopt procedures for information classification, user management and administration, definition of responsible parties and owners of the information to be processed in new technologies to determine and implement information security and cybersecurity controls.
- Establish the management and monitoring of cyber risks and third party risks arising from the implementation of new technologies such as operational, financial, regulatory, organizational and technological risks.
- Include in the business continuity plan the security requirements and controls for resuming operations oriented to automated systems and digital services.
- Oversee compliance of work performed by automated systems, ensuring that these systems adhere to regulatory requirements and organizational policies regarding security.

7.14. Implement cloud security

It is the commitment of the second line to establish the applicable guidelines for services that are exposed to both private and public cloud, and the responsibility of the first line to implement and maintain security on these services, taking into account that, for a public cloud infrastructure, Porvenir must adapt to the security criteria and practices implemented by the provider, ensuring the backup, access and privacy of the information stored there.

7.15. Information Security and Privacy and Cybersecurity Management System Evaluation Model

For the identification of risks and the application of information security and privacy and cybersecurity controls, Porvenir and its subsidiaries adopt and disclose the information security and privacy and cybersecurity assessment model. The purpose of this model is to evaluate the maturity level of the information security and privacy management system and identify opportunities for improvement to strengthen it, based on the domains and controls proposed in the NTC-ISO/IEC 27001:2022 standard, the NTC-ISO/IEC 27701:2020 standard and the NIST Cybersecurity Framework.

7.16. Reports

In order to facilitate compliance monitoring, various management reports will be requested to provide effective support for administration; these must be accurate, understandable, complete, and timely. Likewise, subsidiaries and/or suppliers shall inform Porvenir of any information security and cybersecurity incidents that have significantly affected the confidentiality, integrity, availability and privacy of the company's information at the time they occur, providing a brief description of the incident, its impact and the measures adopted to manage it. Additionally, there must be a consolidated database of information security and cybersecurity incidents classified by type of incident, impact, impact on the information security pillar and remediation plan, and this report must be protected due to the sensitivity of this information.

7.17. Training and Education

Within the induction process of a new employee and at least annually for all employees, a training and/or update on security and privacy of information and cybersecurity should be conducted. Training and coaching can be provided on an ongoing, virtual or face-to-face basis to Porvenir's employees and their subsidiaries, with the purpose of strengthening the concepts and ensuring the continuity and sustainability of the Information Security and Privacy and Cybersecurity Management System. In addition to this, information security and privacy training is provided annually to critical suppliers that access information assets.

7.18. Investigations and Sanctions

Porvenir and its subsidiaries acknowledge that in the event of non-compliance with this policy and other activities derived from it, the persons responsible for non-compliance may be subject to disciplinary action by Porvenir in accordance with internal policies related to the handling of Information Security Incidents. The foregoing, without prejudice to any liability that may arise from non-compliance with the regulations applicable to Information Security and Privacy and Cybersecurity.

8. POLICY VALIDITY AND UPDATE

The General Information Security and Privacy and Cybersecurity Policy will be reviewed annually or when changes are identified in the structure, objectives or any condition that affects the policy, in order to ensure that it is adjusted to the requirements or needs of the Company. Approval of updates or modifications will be made by the Board of Directors after review by the Chairman's Committee and the Information Security and Cybersecurity Committee.

This policy is effective as of the date of publication and the provisions herein are mandatory according to the defined scope.

9. EXTERNAL REGULATIONS

- Basic Legal Circular Financial Superintendency of Colombia (SFC) 029 of 2014 Part I Title IV Chapter V: Minimum requirements for information security and cybersecurity management.
- Basic Legal Circular of the Superintendency of Finance of Colombia (SFC) 029 of 2014 Part I Title III Chapter I: Financial consumer access and information.
- Basic Legal Circular of the Superintendency of Finance of Colombia (SFC) 029 of 2014 For I Title I Chapter VI: Rules regarding the use of cloud computing services.
- Basic Legal Circular of the Superintendence of Finance of Colombia (SFC) 029 of 2014 Part I Title II Chapter I: Channels, means, security and quality in the handling of information in the provision of financial services.
- Law 1581 of 2012. Whereby general provisions are issued for the protection of personal data.
- Sole Circular of the Superintendence of Industry and Commerce (SIC) Title V - Protection of Personal Data.
- External Circular 006 of 2022 (SIC) Processing of personal data for advertising, marketing or commercial prospecting purposes.
- External Circular 001 of 2024 (SIC) Data Subjects and entities supervised by the Superintendence of Industry and Commerce in its role as Personal Data Protection Authority.
- External Circular 002 of 2024 (SIC) Guidelines on the Processing of Personal Data in Artificial Intelligence Systems.
- External Circular 003 of 2024 (SIC) Instructions for corporate administrators in relation to the processing of personal data.

Registry Update

This policy manual has been modified as described below:

No.	Numeral / Title	Description of the Update	Date of Update
1.0	Entire document	This document is created to replace the General Information Security Policy Manual. The policy is updated, extending its scope to include cybersecurity, as well as the commitments of senior management.	November 28, 2018
2.0	Policy	The cloud application is included considering that it is already in a state of implementation and management in the company. External regulations are included, mentioning SFC E.C. 005 of 2019 and SFC E.C. 007 of 2019.	May 10 2023
30	Responsibility of users General Guidelines	Numeral 6 is included. Responsibility of users, mentioning the functions or commitments of the three lines of defense in Porvenir. Numeral 7 is included. General Guidelines mentioning the duties of the Information Security Management System to Porvenir, its subsidiaries and the three lines of defense.	November 22, 2023
4.0	Entire document	The document is modified at a general level in accordance with the transition of the standard to its ISO 27001:2022 version.	July 2024

No.	Numeral / Title	Description of the Update	Date of Update
		1. The General Policy was modified. 2. Senior Management responsibilities are included and modified. 3. General guidelines are included and modified to comply with the applicable requirements of the standard.	
5.0	Entire document 4. POLICY 5. SENIOR MANAGEMENT COMMITMENT 6. RESPONSIBILITIES OF USERS	The document is modified at a general level in accordance with the implementation of ISO 27701:2020, which complements ISO 27001:2022 at the information privacy level. 4. Section 4.2 INFORMATION PRIVACY POLICY in which the specific document where the policy is hosted is mentioned. 5. Senior Management's commitments are modified in accordance with the focus on information privacy. 6. An additional section is included for the first, second and third lines mentioning how the three lines act on the information privacy front. 7. Changes are made to all applicable requirements by making	June 2025

No.	Numeral / Title	Description of the Update	Date of Update
	7. APPLICABLE INFORMATION SECURITY AND PRIVACY REQUIREMENTS 9. EXTERNAL REGULATIONS	emphasis on information privacy. 9. It includes Law 1581 applicable to the protection of personal data, the Sole Circular and External Circulars 006 of 2022, 001 of 2024, 002 of 2024 and 003 of 2024 of the SIC.	