Information Security and CyberSecurity Policy of Prosegur Compañía de Seguridad, S.A.

1. Scope of application

The Board of Directors of Prosegur Compañía de Seguridad, S.A., (" **PCS** " or the " **Company** ") has the non-delegable power to determine its general policies and strategies and, among them, the Information Security and Cybersecurity Policy of the Company and its subsidiaries, (the "**Group** ").

In this regard, the Board of Directors of the Company has approved this Information Security and Cybersecurity Policy, (the "**Policy** "), which sets out the main aspects and commitments of the Company and its Group in the area of Information Security and Cybersecurity.

In accordance with the provisions of the Regulations of the Board of Directors of the Company, the Sustainability, Corporate Governance, Appointments and Remuneration Committee will be responsible for supervising the application of this Policy, periodically evaluating its effectiveness and proposing to the Board of Directors the adoption of appropriate measures for its updating and, where appropriate, resolving any deficiencies.

This Policy applies to all physical locations, personnel, third parties with whom there are contractual relationships and technological assets in the different countries where the Company and its Group are present and those in which it establishes itself as a result of organic and inorganic growth.

2. Object

The commitment to the highest ethical standards and to compliance with the best national and international practices in information security and cybersecurity, together with the values of the Company and its Group, (Proactivity, commitment, value creation, customer focus, transparency, excellence, leadership, teamwork and brand), form the pillars on which the Company and its Group base the protection of its information and the assets associated with its processing and management.

In its commitment to transparency, the rules and main policies that make up the Company's Corporate Governance system, including this Policy, are permanently available to the market and, in particular, to its shareholders and investors, through its corporate website, (www.prosegur.com).

The purpose of this Policy is to establish the basic principles and general framework for the management of Information Security and Cybersecurity, improving its resilience capacity, providing an adequate response to the associated risks and cyber-risks, and preserving at all times the dimensions associated with information and information systems: confidentiality, integrity, availability, authenticity, non-repudiation and traceability.

3. Principles and Development

The Company and its Group, through the establishment of this Policy, undertake to:

- Applicable **regulatory and normative requirements, especially regarding security and protection of personal data.**
- **Define, develop and implement technical and organizational controls,** based on continuous risk assessment**,** to protect the assets and information of the Company and its

Group, as well as customer information to which it has access within the framework of its activities.

- Aligning security with the **business objectives** set by the Company and its Group.
- **Establish a risk management strategy and process**.
- **Define the general guidelines** for action to prevent threats and **react to** information security incidents.
- **Maintain contact with the authorities** through the appropriate channels.
- **Manage the assets** of the Company and its Group from their acquisition, through their identification, classification, prioritization, custody, transport and disposal.
- **Keep facilities protected** from physical and environmental threats with security controls.
- **Integrate information security and cybersecurity** from the design stage in all projects, systems, and new services.
- **Conduct security audits** to review compliance over time, as well as certify our systems and products **according to the main standards.**
- **Monitor the systems and networks of the Company and its Group** to prevent unauthorized access, third-party attacks and other causes that may compromise them, relying on the exchange and use of intelligence on cyber threats.
- **Ensuring digital operational resilience and business continuity** in the face of disruptive security incidents.
- **To demand and safeguard compliance with information security standards** by suppliers and third parties.
- **Inform and raise awareness** among all staff about the information security strategy, creating an information security culture with staff, partners, and suppliers.
- **Promote the continuous improvement** of the Information Security and Cybersecurity Management System, evaluating its effectiveness and adapting it to the evolution of cyber threats.

All of the above will be applied in accordance with a risk-based approach and the principle of proportionality, taking into account the criticality of the Group's assets, processes and companies, as well as the potential operational, financial, regulatory and reputational impact.

4. Approval, dissemination and knowledge of this Policy

The Company's Board of Directors will approve any other corporate rules, policies or programs that it considers necessary or appropriate for the proper functioning of the Company and its Group.

This Policy will be published on the corporate website and the Company's intranet, and may be included in training materials for staff and in additional dissemination activities.

5. Preparation and Approval

Owner:	Prosegur Global CISO		
Reviewed by:	Prosegur Global CISO	Corporate Legal Area	
Approved by:	Board of Directors of Prosegur Compañía de Seguridad, S.A.	Date:	30/04/2026

***