00-PO-02 INFORMATION SECURITY POLICY

Elaborated	Revised	Approved
25/09/2024	03/10/2024	03/10/2024

REVISION CONTROL

VERSION	SECTIONS MODIFIED	REASON FOR CHANGE	DATE
1	All	First Version	25/03/2018
2	All	Unification Policy Information Security and Quality Policy	01/03/2022
3	All	Adaptation of the ENS Segregation of the policy of Quality	25/09/2024

Index

1. PRINCIPLES OF THE SYSTEM.....4
2. LEGAL AND REGULATORY FRAMEWORK 5
3. ROLES AND RESPONSIBILITIES 6
4. APPROVAL.....8

1. PRINCIPLES OF THE SYSTEM

Ethics Channel SL and BII International Associates (hereinafter GAT GROUP), as a company dedicated to the implementation and maintenance of non-compliance reporting channels for companies on the web, as well as the provision of services for the reception and primary management of such reports, assumes its commitment to the security of information, committing itself to the proper management of the same, in order to offer all its stakeholders the best guarantees regarding the security of the information used. In view of the above, the Management establishes the following information security objectives:

- Provide a framework for building resilience to respond effectively to critical security situations.
- Ensure the rapid and efficient recovery of services in the event of any physical disaster or contingency that might occur and jeopardise the continuity of operations.
- Prevent information security incidents to the extent technically and economically feasible, as well as mitigate information security risks generated by our activities.
- Ensuring confidentiality, integrity, availability, authenticity and traceability of information

In order to achieve these objectives it is necessary to:

- **Continuously improve** our information security system.
- Comply with applicable legal requirements and any other requirements to which we subscribe as well as our commitments to customers, and continuously update them.
- Identify potential threats, as well as the impact on business operations that such threats, should they materialise, may cause.
- Preserve the interests of its key stakeholders (customers, shareholders, employees and suppliers), reputation, brand and value creation activities.
- Working together with our suppliers and subcontractors to improve IT service delivery, service continuity and information security, leading to greater efficiency in our business.
- Assessing and guaranteeing the **technical competence of staff**, as well as ensuring adequate motivation of staff to participate in the continuous improvement of our processes, by providing adequate training and internal communication for them to develop good practices defined in the system.

- Ensure the **correct state of the facilities and the** appropriate **equipment**, so that they are in line with the activity, objectives and goals of the company.
- Ensure a continuous **analysis** of all **relevant processes**, establishing the relevant improvements in each case, depending on the results obtained and the objectives set.
- Structure our management system in a way that is easy to understand. Our management system has the following structure:

2. LEGAL AND REGULATORY FRAMEWORK

The legal and regulatory framework in which we carry out our activities is:

- *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of*

  27 April 2016 on the protection of individuals with regard to the protection of individuals with regard to the processing of personal data and on the free movement of such data
- *Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights.*
- *Royal Legislative Decree 1/1996 of 12 April 1996, Law on Intellectual Property.*
- *Royal Decree-Law 2/2018, of 13 April, amending the revised text of the Intellectual Property Law*
- *REGULATION (EU) No 910:2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of*

  23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (European eIDAS Regulation).
- *Occupational Risk Prevention Law 31/1995 of 8 November 1995 and Royal Decree 39/1997 of 17 January 1997, approving the Prevention Services Regulations.*

- *Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce (LSSI-CE).*
- *RD-ley 13/2012 of 30 March, cookies law.*
- *Royal Legislative Decree 1/1996, of 12 April 1996, approving the revised text of the Intellectual Property Law, regularising, clarifying and harmonising the legal provisions in force on the matter.*
- *Resolution of 7 October 2016, of the Secretary of State for Public Administrations, approving the Technical Security Instruction on the Security Status Report.*
- *Resolution of 13 October 2016, of the Secretary of State for Public Administrations, approving the Technical Security Instruction in accordance with the National Security Scheme.*
- *Resolution of 27 March 2018, of the Secretary of State for Public Function, approving the Technical Security Instruction on Auditing the Security of Information Systems.*
- *Resolution of 13 April 2018, of the Secretary of State for Public Function, approving the Technical Security Instruction on Security Incident Notification.*
- *Royal Decree 311/2022, of 3 May, regulating the National Security Scheme*
- *UNE-EN ISO/IEC 27001:2017 Information Security Management System*

3. ROLES AND RESPONSIBILITIES

The management of our system is entrusted to the Management Manager and the system will be available in our information system in a repository, which can be accessed according to the access profiles granted under our current access management procedure.

These principles are assumed by the Management, which has the necessary means and provides its employees with sufficient resources to comply with them, and they are set out and made public through this Integrated Management Systems Policy.

The security roles or functions defined in ESRI are

Function	Duties and responsibilities
Responsible for the information	❑ Making decisions relating to the information processed
Responsible for services	❑ Coordinate the implementation of the system ❑ Continuous improvement of the system
Responsible for security	❑ Determining the adequacy of technical measures ❑ Providing the best technology for service
Responsible for the system	❑ Coordinate the implementation of the system ❑ Continuous improvement of the system

Address	❑ Providing the necessary resources for the system ❑ Leading the system

This definition is completed in job profiles and system documents.

The procedure for their appointment and renewal shall be ratification in the security committee.

The committee for security management and coordination is the most responsible body within the information security management system, so that all major security-related decisions are agreed by this committee. The members of the information security committee are:

- ❑ Responsible for the information.
- ❑ Responsible for services.
- ❑ Responsible for security.
- ❑ Responsible for the system.
- ❑ Management Company (partner-managers)

These members are appointed by the committee, which is the only body that can appoint, renew and dismiss them.

The safety committee is an autonomous, executive body with autonomy in decision-making and does not have to subordinate its activity to any other element of our company.

This policy is complemented by the other policies, procedures and documents in place to develop our management system.

4. APPROVAL

In Madrid, 03 October 2024

Gertrudis Alarcón, CEO