CORPORATE COMPLIANCE POLICY

CORPORATE COMPLIANCE SYSTEM

JULY 2025

TABLE OF CONTENTS

1. CONTEXT OF THE ORGANISATION

1.1. HISTORICAL AND ORGANISATIONAL CONTEXT

SERVEIS I ADMINISTRACIONS MASERGRUP S.L.U. (hereinafter, "MASERGRUP"), is a family-owned industrial group that was founded in 1997 in Reus by entrepreneur Xavier Martínez i Serra. The Group currently operates as a producer in the following sectors: industrial, real estate, healthcare, food, and services.

Since its foundation, MASERGRUP has grown and diversified its activities, remaining faithful to its commitment to innovation, society and the environment.

1.2. ORGANISATIONAL CHART OF THE PARENT COMPANY

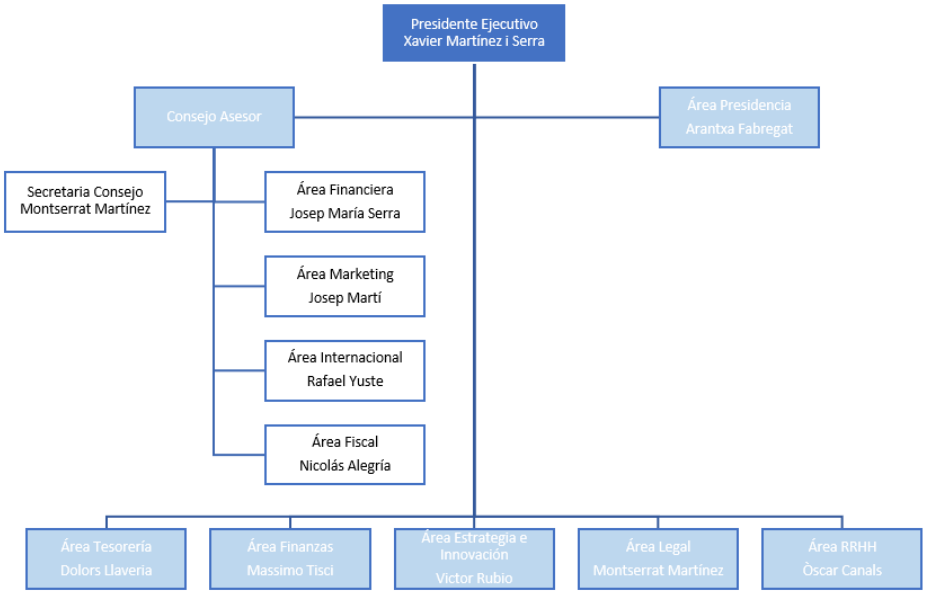
The MASERGRUP holding company currently comprises the following companies:

1.3. DIVISIONAL ORGANISATION CHART

The registered office and headquarters of MASERGRUP are located at Reus, C/ Joan Fuster 15, 43206 (Tarragona). However, the companies that make up the Group currently have a presence in the following countries:

1.4. FUNCTIONAL ORGANISATION CHART

At the functional level, MASERGRUP is organised as follows:



2. INTRODUCTION TO THIS POLICY

2.1. REGULATORY CONTEXT

On 23 December 2010, Organic Law 5/2010 of 22 June reforming the Criminal Code came into force, recognising for the first time in Spanish law the true criminal liability of legal persons, making them direct subjects of criminal law capable of committing crimes and, therefore, liable to real penalties.

This reform established the offences applicable to legal persons and their requirements, as well as the surveillance and control measures for their prevention and detection as the express basis for the mitigation of criminal liability.

Thus, legal persons may be held criminally liable:

a) For offences committed in their name or on their behalf, and for their direct or indirect benefit, by their legal representatives or by those who, acting individually or as members of a body of the legal person, are authorised to take decisions on behalf of the legal person or have powers of organisation and control within it.

b) For offences committed in the exercise of social activities and on behalf of and for the direct or indirect benefit of the legal person, by persons who, being subject to the authority of the natural persons referred to in the previous paragraph, have been able to carry out the acts because of a serious breach by the latter of their duties of supervision, monitoring and control of their activity, taking into account the specific circumstances of the case.

On 1 July 2015, Organic Law 1/2015 came into force, which enshrined the aforementioned regime, expressly admitting the exemption from liability for legal persons in the event that the six basic elements that, in accordance with the provisions of Article 31 bis of the Criminal Code, must be present in an organisational and management model in order to assess its exonerating potential, are met.

In May 2017, the UNE 19601 standard was published, setting out requirements and guidance for the use of *Corporate Compliance* Programmes. It developed the six elements required by the Criminal Code into ten basic points that criminal *compliance* systems implemented in legal entities must comply with to be considered effective and deserving of exemption.

Likewise, ISO 37301 on *Compliance* Management Systems was approved in April 2021, and UNE-ISO 37001 on Anti-Bribery Management Systems was approved in April 2017, completing the essential reference framework for the creation of *Corporate Compliance* programmes.

On 23 October 2019, Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report on breaches of Union law was approved, which was transposed into Spanish law through the approval, on 20

February 2023, of Law 2/2023, of 20 February, regulating the protection of persons who report regulatory infringements and the fight against corruption.

On the other hand, it should be borne in mind that *compliance* systems are not only an instrument for potentially exempting legal persons from criminal liability but must be designed as a mechanism to promote a genuine culture of ethics and corporate compliance.

In this regard, on 10 June 2020, the National Commission for Markets and Competition ("CNMC") published a guide to compliance programmes in relation to the defence of competition ("CNMC Guide"). The CNMC Guide identifies seven assessment criteria for the implementation of effective competition compliance programmes: (i) the involvement of the company's administrative bodies and/or senior management; (ii) effective training; (iii) the existence of an Ethics Channel; (iv) the independence and autonomy of the person responsible for designing and monitoring compliance policies; (v) the identification of risks and the design of protocols or control mechanisms; (vi) the design of internal procedures for handling complaints and detecting infringements; and (vii) the design of a transparent and effective disciplinary system.

2.2. ETHICAL COMMITMENT

Beyond the purely legal provisions relating to regulatory compliance, the company has made a genuine ethical commitment that affects all members of the company, without exception, and which is embodied in the following principles, listed below by way of example:

(i) Regulatory compliance is the basic operating principle of the company, to which the business is subject.

(ii) The decision-making process at all levels is geared towards compliance with and observance of the highest ethical standards.

(iii) Senior management promotes, by example, a genuine commitment to a culture of compliance and the prevention of crime.

(iv) There is zero tolerance for regulatory and ethical non-compliance, and this principle applies at all levels of the organisation.

(v) A culture of respect for the law must be a source of inspiration for action at all levels of the company.

(vi) There are adequate and effective instruments in place to prevent crime and promote a genuine ethical culture within the company.

2.3. PURPOSE OF THE POLICY

As a result of the ethical commitment undertaken by MASERGRUP and in the aforementioned regulatory context, a *Corporate Compliance* System has been

implemented, aimed at reviewing the company's control systems and implementing new measures to prevent and control the commission of crimes within the company.
The purpose of this *Compliance* Policy is to describe the prevention programme implemented in the company, without including details of all the internal regulations on the subject. For details of these regulations, please refer to the specific policies, procedures and processes that make up the *compliance* system.

The main objectives to be achieved through the development of this Policy are as follows:

(i) Firstly, the Policy sets out how the organisation's *Corporate Compliance* System works, establishing the guidelines drawn up by the company for the prevention, detection and management of criminal risks. In this way, all the regulations developed within the organisation in relation to criminal *compliance* share the same objectives and basic characteristics as defined in this Policy.

(ii) Secondly, this Policy serves to inform MASERGRUP employees and new recruits of the organisation's position on the fight against crime and the behaviour expected of all members of the organisation. It also aims to publicise the company's policies and protocols that should be consulted in case of doubt as to whether the intended conduct is permitted, and to inform about the procedure to be followed to bring to the company's attention any criminal behaviour that has been committed, or is being committed, within the company and of which it is aware.

(iii) Thirdly, this Policy allows the organisation to inform interested third parties of the main features of the criminal prevention model implemented and how the organisation is committed to regulatory compliance through this model.

(iv) Finally, the Policy demonstrates an organisational culture of respect for the law and the existence of reasonable and proportionate measures to prevent, detect and manage criminal risks affecting the organisation, all in accordance with the requirements of the Criminal Code and UNE 19601.

2.4. OBJECTIVE SCOPE

This Policy defines the characteristic features of MASERGRUP's *Corporate Compliance* System, and therefore the elements that comprise it are aimed at preventing, detecting and managing only those risks for which the company could be criminally liable, in accordance with Article 31 bis of the Criminal Code, or administratively liable in accordance with the Treaty on the Functioning of the European Union ("TFEU") and Law 15/2007 of 3 July on the Defence of Competition ("LDC").

Compliance risks arising from *compliance* obligations other than those established (i) in the Criminal Code and the non-criminal regulations to which it refers to complete the criminal offence and (ii) in competition law are excluded from the programme.

2.5. INTERESTED PARTIES AND SUBJECTIVE SCOPE

With regard to the subjective scope and interested parties[1] , this Policy (and, accordingly, the entire *Corporate Compliance* System implemented by MASERGRUP) is addressed to all employees and managers of the Group, regardless of their position and geographical location, as well as to third parties related to MASERGRUP or the companies that comprise it, so that they may be aware of the company's position on non-compliance, understand its ethical commitments, and adhere to them.

For this reason, all members of MASERGRUP, and all third parties related to it, must commit to complying with its *Corporate Compliance* System, as well as to complying with the values and principles of conduct that the Group has adopted as a guide for action.

2.6. RESPONSIBILITY

All members of the company are responsible for complying with the provisions of this Policy and all internal regulations that form part of the *Corporate Compliance* System. Department heads must disseminate the content of this Policy among the staff under their responsibility.

2.7. APPROVAL, UPDATING AND DISCLOSURE

This Policy has been approved by the Sole Administrator and President of MASERGRUP, in accordance with the provisions of the Annex "**Approval and Amendments**" and shall remain in force until it is amended or replaced by another version.

In addition, the policy will be available on the MASERGRUP Intranet, so that it is accessible to both employees and all interested parties who, due to their relationship with the company, need to be aware of its content.

[1] It is based on the definition of "Interested Party" contained in ISO 37301, on Compliance Management Systems, and in UNE-ISO 37001, on Anti-Bribery Management Systems, in which an interested party is understood to be any "person or organisation that can affect, be affected by, or perceive itself as affected by a decision or activity".

This Policy, and the entire MASERGRUP *Corporate Compliance* System, will be reviewed every two years (alternate years), as well as whenever there are relevant regulatory or jurisprudential changes, changes in the structure or activity of the company, breaches of its regulations, or for other reasons, which will be duly justified, as decided by the Sole Administrator or the *Compliance Officer* himself.

Finally, whenever there is a change in the *Corporate Compliance* System for any of the reasons set out in the previous paragraph, and this involves the modification of any of the documents that comprise it (policies, protocols, and implementing regulations), such notification shall be communicated to all members of the company and third parties who, by reason of their relationship with it, should be aware of it, and the corresponding document shall be sent to them in its most up-to-date version.

3. OFFENCES THAT MAY GIVE RISE TO CRIMINAL LIABILITY FOR MASERGRUP

The identification of criminal risks forms the basis for the implementation of MASERGRUP's *Corporate Compliance* System and enables the company to allocate resources and establish appropriate processes to manage the risks identified.

The directors of each area are responsible for identifying, analysing, controlling, monitoring and reviewing criminal risks within their sphere of competence, ensuring that the necessary controls are in place to prevent and manage them, with the support and advice of *the Compliance Officer*.

If the head of an area or department considers that there is a criminal risk in their sphere of activity that is not currently covered, or that an identified criminal risk is not adequately mitigated, they must immediately contact the *Compliance Officer* in order to assess the situation and implement the appropriate corrective measures, if necessary.

3.1. METHODOLOGY

The criminal risk management methodology followed by the company consists of the following eight elements:

ELEMENTS FOR CRIMINAL RISK MANAGEMENT	
1. DETERMINATION OF CONTEXT AND SCOPE	› The company's risk management has begun with: o **Determining the external and internal factors** that are relevant to achieving the *compliance* objective, such as the company's structure, activity and regulatory obligations. o Deciding on the **scope of the risks** to be addressed. › These risks are criminal offences for which MASERGRUP may be held criminally liable, in accordance with Articles 31 bis et seq. of the Criminal Code, as well as for the ancillary consequences provided for in Article 129 of the Criminal Code.
2. RISK IDENTIFICATION	› Once the context and scope have been defined, the directors of each department, with the assistance of *the Compliance Officer*, have reflected on the activities carried out by their team in order to **identify any criminal risks (within the scope) that could arise** in the performance of their duties.

3. RISK ANALYSIS	➢ The risks identified have been analysed taking into account: o The **probability** of the risk faced by MASERGRUP materialising; and o The **impact** and/or severity of the consequences of its materialisation. ➢ The result of adding the probability of the risk materialising and its impact is known as the **gross risk**.
4. RISK ASSESSMENT	➢ Therefore, we propose incorporating a series of **controls and measures into the company** which, depending on their design and effectiveness, will mitigate the identified risk to a greater or lesser extent. ➢ The gross risk reduced by the assessment of existing controls and measures will result in what is known as **net risk**. ➢ This allows the company to allocate resources on a priority basis to mitigating the risks with the highest ratings and, ultimately, to apply monitoring and corrective measures to all identified risks in order to meet *compliance* objectives.
5. RISK CONTROL	➢ The criminal risks identified must be controlled through the implementation of the controls finally put in place, aimed at **risk prevention, detection and management**.
6. MONITORING	➢ The directors of each department, together with MASERGRUP's *Compliance Officer*, shall periodically supervise and verify that criminal risks are being **properly controlled** and that the *compliance* objective is being met.
7. COMMUNICATION AND TRAINING	➢ MASERGRUP will make an Internal Information System ("SII") available to all its members with the aim of: o There is proper dissemination and understanding of criminal risks and controls within the framework of the *Corporate Compliance* System. o To be able to communicate well-founded suspicions of non-compliance or propose or suggest improvements to the System or the company.
8. SYSTEM REVIEW	➢ The directors of each department and the MASERGRUP *Compliance Officer* **will** periodically **review the identification, analysis and assessment of criminal risks**, particularly when any of the following circumstances arise: o Significant changes in the company's structure or activities. o Breaches of criminal *compliance*. o Appearance of relevant case law or legislative changes, for which the company must be duly updated and advised.

3.2. CRIMES THAT MAY GIVE RISE TO CRIMINAL LIABILITY FOR LEGAL ENTITIES

Under Article 31 bis of the Criminal Code, legal entities may be held criminally liable for offences expressly provided for in the Criminal Code. The current **list of offences** for which a legal entity may be held criminally liable is as follows:

- Illegal trafficking of organs (Art. 156 bis of the Criminal Code).
- Crime against moral integrity (Art. 173 of the Criminal Code).
- Crime of concealing a corpse (Art. 173.1 of the Criminal Code).
- Crime of human trafficking (Art. 177 bis of the Criminal Code).
- Sexual access (Art. 183 of the Criminal Code)
- Offences of prostitution, sexual exploitation and corruption of minors (Art. 187 to 189 bis of the Criminal Code).
- Offences relating to the discovery and disclosure of secrets (Art. 197 to 197 quinquies of the Criminal Code).
- Fraud (Articles 248 to 251 bis of the Criminal Code).
- Obstruction of justice (Articles 257 to 258 ter of the Criminal Code).
- Punishable insolvency (Articles 259 to 261 bis of the Criminal Code).
- Computer crimes (Articles 264 to 264 quater of the Criminal Code).
- Offences against intellectual and industrial property (Articles 270 to 277 of the Criminal Code).
- Discovery and disclosure of trade secrets (Article 278 of the Criminal Code).
- Misleading advertising (Article 288 of the Criminal Code).
- Money laundering (Articles 301 and 302 of the Criminal Code).
- Illegal financing of political parties (Art. 304 bis and ter of the Criminal Code).
- Offences against the Public Treasury and Social Security (Art. 305 to 310 of the Criminal Code).
- Subsidy fraud (Art. 310 bis of the Criminal Code).
- Accounting offences (Art. 310 bis of the Criminal Code).
- Offences against the rights of foreign nationals (Art. 318 bis of the Criminal Code).
- Corruption in business (Art. 286 bis to quater of the Criminal Code).
- Offences against land use planning and urban development (Art. 319 of the Criminal Code).
- Offences against the environment (Articles 325 to 328, 339 and 340 of the Criminal Code).
- Animal abuse (Article 340 bis of the Criminal Code).
- Offences relating to nuclear energy and ionising radiation (Article 343 of the Criminal Code).
- Crimes caused by explosives and other agents (Art. 348 of the Criminal Code).
- Crimes against public health (Art. 366 of the Criminal Code).
- Drug trafficking (Art. 368 bis of the Criminal Code).
- Crime of forgery of credit cards, debit cards and traveller's cheques (Art. 399 bis of the Criminal Code).
- Bribery (Art. 424 of the Criminal Code).
- Influence peddling (Art. 428 to 430 of the Criminal Code).
- Embezzlement (Art. 432 to 435 of the Criminal Code).
- Corruption of foreign officials (Art. 427 bis of the Criminal Code).
- Hate crime and glorification (Art. 510 bis of the Criminal Code).
- Financing of terrorism (Art. 578 of the Criminal Code).
- Smuggling (Art. 1 and 2 of LO 12/1995 on the suppression of smuggling).

In addition to the penalties that may be imposed on legal entities, Article 129 of the Criminal Code provides for the application of a series of **additional consequences,** which may be applied when committed within, with the collaboration of, through or by means of companies, organisations, groups or any other type of entity or group of persons which, due to their lack of legal personality, are not covered by Article 31 bis, adding to the above the offences set out below.

However, it should be noted that, according to the literal interpretation of the provisions, legal persons cannot be punished under Article 129 of the Criminal Code, nor can any exemption be obtained based on the existence or absence of a *Corporate Compliance* System.

In this regard, there is case law demonstrating that the accessory consequences of Article 129 of the Criminal Code have been imposed on entities with legal personality, as in Supreme Court Ruling 162/2019 of 26 March and Supreme Court Ruling 121/2017 of 23 February.

In this context, and insofar as a penalty may in some way be imposed on the legal entity (whether criminal or not), it has been considered appropriate to analyse the offences under Article 129 of the Criminal Code, which are listed below, as they could give rise to the imposition of additional penalties on MASERGRUP:

- Genetic manipulation offences (Art. 162 of the Criminal Code).
- Offence of price fixing in public tenders and auctions (Art. 262 of the Criminal Code).
- Offence of refusal to cooperate with inspections (Art. 294 of the Criminal Code).
- Offences against workers' rights (Art. 318 of the Criminal Code).
- Counterfeiting currency and stamped documents (Art. 386, 387 of the Criminal Code).
- Offence of unlawful association (Art. 515 of the Criminal Code).
- Offences relating to criminal organisations and groups (Art. 570 bis and ter of the Criminal Code).
- Offences relating to terrorism and terrorist organisations and groups (Art. 571 to 579 of the Criminal Code).

3.3. OFFENCES FOR WHICH NO RISK OF COMMISSION IS DETECTED WITHIN MASERGRUP

In accordance with Article 31 bis of the Criminal Code, and in accordance with the activities carried out by the company, as well as its corporate structure, the offences that could give rise to criminal liability for the legal entity are not currently expected to result in MASERGRUP being held criminally liable, as it is considered that such offences are not likely to generate any direct or indirect benefit for the company. These offences are listed below:

- Illegal organ trafficking (Art. 156 bis of the Criminal Code).
- Concealment of a corpse (Art. 173.1 of the Criminal Code).
- Human trafficking (Art. 177 bis of the Criminal Code).
- Crimes of prostitution, sexual exploitation and corruption of minors (Articles 187 to 189 bis of the Criminal Code).
- Illegal financing of political parties (Articles 304 bis and ter of the Criminal Code).
- Crime of animal abuse (Article 340 bis of the Criminal Code).

- Offences relating to nuclear energy and ionising radiation (Art. 343 of the Criminal Code).
- Offences caused by explosives and other agents (Art. 348 of the Criminal Code).
- Drug trafficking (Art. 368 bis of the Criminal Code).
- Offence of forgery of credit cards, debit cards and traveller's cheques (Art. 399 bis of the Criminal Code).
- Embezzlement (Art. 432 to 435 of the Criminal Code).
- Hate crimes and glorification (Art. 510 bis of the Criminal Code).
- Terrorist financing (Art. 578 of the Criminal Code).

Similarly, and in relation to the accessory consequences provided for in Article 129 of the Criminal Code, in accordance with the activity carried out at MASERGRUP, none of the following crimes have been detected as likely to materialise, as they have not been considered to generate any direct or indirect benefit to the company:

- Genetic manipulation offences (Art. 162 of the Criminal Code).
- Offences relating to price fixing in public tenders and auctions (Art. 262 of the Criminal Code).
- Offences relating to unlawful association (Art. 515 of the Criminal Code).
- Offences relating to criminal organisations and groups (Art. 570 bis and ter of the Criminal Code).
- Offences relating to terrorist organisations, groups and terrorism (Art. 571 to 579 of the Criminal Code).
- Counterfeiting of currency and stamped documents (Art. 386, 387 of the Criminal Code).

3.4. CRIMES WHOSE RISK OF OCCURRENCE IS DETECTED IN MASERGRUP

In view of the above, the crimes listed in Article 31 bis of the Criminal Code, which, given the nature of the company's activities, could potentially be committed and therefore require MASERGRUP to take special preventive measures (i.e., implementation of *compliance* measures and controls), are as follows:

- Crimes against moral integrity (Art. 173 of the Criminal Code).
- Sexual harassment (Art. 184 of the Criminal Code).
- Crimes relating to the discovery and disclosure of secrets (Art. 197 to 197 quinquies of the Criminal Code).
- Fraud (Articles 248 to 251 bis of the Criminal Code).
- Obstruction of justice (Articles 257 to 258 ter of the Criminal Code).
- Punishable insolvency (Articles 259 to 261 bis of the Criminal Code).
- Computer damage (Articles 264 to 264 quater of the Criminal Code).
- Offences against intellectual and industrial property (Articles 270 to 277 of the Criminal Code).
- Discovery and disclosure of trade secrets (Art. 278 of the Criminal Code).
- Corruption in business (Art. 286 bis to quater of the Criminal Code).
- Misleading advertising (Art. 288 of the Criminal Code).
- Money laundering (Art. 301 and 302 of the Criminal Code).
- Offences against the Public Treasury and Social Security (Articles 305 to 310 of the Criminal Code).
- Subsidy fraud (Article 310 bis of the Criminal Code).
- Accounting offences (Article 310 bis of the Criminal Code).
- Offences against the rights of foreign nationals (Article 318 bis of the Criminal Code).

- Offences against land use planning and urban planning (Art. 319 of the Criminal Code).
- Offences against the environment (Art. 325 to 328, 339, 340 of the Criminal Code).
- Offences against public health (Art. 365 of the Criminal Code).
- Bribery (Art. 424 of the Criminal Code).
- Corruption of foreign officials (Art. 427 bis of the Criminal Code).
- Trafficking in influence (Art. 428 to 430 of the Criminal Code).
- Smuggling (Art. 1 and 2 of Organic Law 12/1995 on the suppression of smuggling).

On the other hand, the offences that may entail the additional consequences provided for in Article 129 of the Criminal Code and whose risk of commission would also be possible at MASERGRUP are as follows:

- Offence of refusal to cooperate with inspections (Art. 294 of the Criminal Code).
- Offence against workers' rights (Art. 318 of the Criminal Code).

4. *COMPLIANCE* CONTROLS

The *Corporate Compliance* System implemented at MASERGRUP consists of a set of internal regulations, procedures and processes whose purpose is to prevent, detect and manage the criminal risks identified in the organisation. These elements are referred to as *compliance* controls.

The main *compliance* control from which all others derive, and which acts as the cornerstone of expected behaviour within the organisation, is the **Code of Ethics**. Drawn up with the aim of developing the values and principles that should guide daily activities, and approved by the Sole Director, it is the highest-ranking rule in the criminal risk management system.

The Code of Ethics is supplemented by **other** high-level standards that apply to all risks managed by the company's *Corporate Compliance* System, such as this **Criminal *Compliance* Policy** and the **Internal Information System Policy** ("SII").

At a third level are those policies and procedures that address a specific set of risks. In this category, the following controls stand out:

- **Telematic Code**: clearly and transparently specifies the use that must be made of corporate telematic means during the term of the employment relationship and upon its termination.

- **Leaflet on the use of IT tools**: complementary to the Telematic Code, which sets out in a clear, simple and educational manner the main rules and guidelines to be followed for the proper use of the IT resources and tools that the company makes available to its employees.

- **Anti-Corruption Policy**: develops the principles and values contained in the Code of Ethics in relation to the company's commitment to preventing corruption. In this regard, it establishes criteria and guidelines for the prevention of corruption and conflicts of interest that may arise in the ordinary activities carried out by personnel or persons linked to MASERGRUP, whether with other individuals (private corruption) or with public officials (public corruption).

- **Protocol for the prevention of and response to harassment** aims to establish the necessary parameters for action to ensure the fundamental right of all workers to be treated with respect and dignity.

- **Money Laundering and Terrorist Financing Prevention Manual**: identifies a series of due diligence measures designed to make economic transactions with suppliers, customers and other counterparties more transparent, to prevent conduct that could be classified as money laundering and/or terrorist financing. This policy includes the *KYC procedure,* which consists of the procedure to be followed by the company when contracting with customers to prevent such

business relationships from being used for illegal purposes, such as money laundering.

- **D Responsible supplier declaration on regulatory compliance:** this sets out the commitment made by the company's suppliers to comply with its principles, values and ethical guidelines, as well as their commitment to developing a culture of compliance with competition law.

5. THE CONTROL STRUCTURE

All members of MASERGRUP are bound by and committed to their criminal *compliance* obligations, from the Sole Administrator to the most recently hired employees.

This is reflected in the assignment of different responsibilities in the management of the criminal risk management system, according to the hierarchy of the members of the company, which is structured as follows.

5.1. THE SOLE ADMINISTRATOR

The Sole Administrator and President of MASERGRUP, together with senior management, are the main drivers of the Criminal Risk Management System, acting with leadership in their commitment to the company's values and promoting a culture of compliance with the law, internal regulations and the voluntary commitments stipulated by the organisation.

The Sole Administrator is ultimately responsible for maintaining and improving the Criminal Risk Management System and must ensure that it has adequate and sufficient financial, material and human resources for its effective operation.

Thus, the Administrator's specific duties in *Corporate Compliance* include the following:

(i) Assigning sufficient resources for the establishment, implementation, development, evaluation, maintenance and improvement of the *Corporate Compliance* System.

(ii) Ensuring the existence and proper implementation of communication channels for reporting issues relating to the *Corporate Compliance* System.

(iii) Align the company's strategic, operational and commercial goals with its *corporate compliance* obligations.

(iv) Establish a disciplinary regime sufficient to ensure accountability and responsibility in cases of regulatory non-compliance.

(v) Integrate regulatory compliance as a parameter for evaluating the performance of company members.

To ensure the proper fulfilment of the above commitments, the Administrator has delegated functions to the *Compliance Officer*.

5.2. THE COMPLIANCE OFFICER

The *Compliance Officer* is responsible for promoting the establishment of *compliance* measures that reasonably prevent, detect and manage identified criminal risks; periodically reviewing the Programme to ensure that it remains effective; and implementing, promoting and managing the SII through which members of the organisation can submit questions, suggestions and reports of non-compliance.

The *Compliance Officer* shall be responsible for the continuous improvement, supervision and review of the Criminal Risk Management System and, where deemed necessary, shall ensure that appropriate professional advice is available. He also reports periodically to the Sole Administrator on the actions taken in *Corporate Compliance*.

The position of *Compliance Officer* is currently held by **Mr Xavier Grau Beltran.**

The main duties assigned to the *Compliance Officer* include the following:

(i) Identifying activities in which *compliance* risks that must be prevented and managed by the company may arise, considering the causes and sources of possible breaches, as well as the seriousness of their consequences and the likelihood of their occurrence.

(ii) Promoting, monitoring and ensuring effective compliance with the values, principles and rules of conduct established in the company's Code of Ethics.

(iii) To approve, develop, coordinate and disseminate policies, codes, procedures and/or internal controls, as well as to promote all necessary training activities related to the prevention of *compliance* risks, which by their nature do not require the prior approval of the Sole Director.

(iv) Ensure that there is access to appropriate professional advice for the establishment, implementation and maintenance of the *compliance* management system.

(v) Enable and manage an Internal Information and Documentation System for *compliance* ("SII"), through which all employees can confidentially report breaches in this area. The SII Manager, in their dual role as the company's *Compliance Officer*, must also implement processes to manage the information received through the SII.

(vi) Direct and document the investigation of any breach of the established measures, as Head of the IIS, to prevent possible *compliance* breaches within the company and take appropriate disciplinary measures where necessary.

(vii) Periodically evaluate the effectiveness of the *compliance* risk management system and promote any changes that may be necessary because of breaches detected since the last control, new obligations introduced in the regulatory environment and/or changes in the structure, composition or activity of the company.

(viii) Report regularly to the company's Sole Administrator on the progress and results of their activities as *Compliance Officer*. The frequency of the regular report shall be annual, through the preparation of an Annual Report, without prejudice to the *Compliance Officer* being able to report to the Sole Administrator in all cases where they deem it necessary, or when requested to do so by the Sole Administrator.

5.3. SENIOR MANAGEMENT

MASERGRUP's management also assumes responsibilities and functions in the area of *Corporate Compliance* within their respective areas of responsibility. These functions include the following:

(i) Cooperating and collaborating to ensure compliance with the *Corporate Compliance* System*,* encouraging all employees within their area of influence to do the same.

(ii) Monitoring and supervising that all employees under their control comply with their assigned functions in terms of regulatory compliance.

(iii) Properly identifying and communicating the risks of regulatory non-compliance in the operations and activities they carry out.

(iv) Integrate regulatory compliance commitments and obligations into the business practices and procedures carried out in their areas of control and responsibility.

(v) Assist and support employee training activities in the area of *corporate compliance.*

(vi) Work to raise awareness among all employees of their regulatory compliance obligations.

(vii) Encourage all company employees to share their concerns through the *Compliance* Consultation Channel*,* supporting them in their approach and avoiding any type of retaliation for doing so.

(viii) Proactively participate in the resolution of all *compliance* issues and incidents that may arise.

(ix) Work to ensure that whenever a need for improvement or correction of the *Corporate Compliance* system is detected, the necessary measures are effectively implemented to remedy the situation.

In addition, senior management will prepare an annual report containing the results and conclusions reached after reviewing the company's *Corporate Compliance* system and its anti-corruption plan.

5.4. OPERATIONAL MANAGEMENT

The organisation's employees are responsible for identifying, analysing and assessing criminal risks within their area of competence and for ensuring that the necessary *compliance* measures are in place to prevent and manage them.

Professionals are the ones who best know the activity of their respective fields and are in the best position to detect the criminal risks that may arise in the course of their work, as well as to assess the suitability and effectiveness of existing measures to address them. For this reason, those responsible for operational management will report periodically to *the Compliance Officer* on the criminal risks affecting their area of competence.

Similarly, those responsible for operational management will receive support in the exercise of their *compliance* functions from the *Compliance Officer*.

In turn, members of the organisation are responsible for understanding, observing and complying with the law, internal regulations and voluntary commitments stipulated by the organisation. All of them must behave in accordance with the Code of Ethics and report any breach thereof to the company through the designated SII.

6. COMMUNICATION, TRAINING AND ACCESSIBILITY

At MASERGRUP, we consider it essential that members of the organisation are aware of, understand and have access to all internal regulations that they are required to apply and comply with.

That is why, for the Criminal Risk Management System to function effectively, communication, training and access to documentation are essential.

6.1. COMMUNICATION

MASERGRUP undertakes to communicate all policies, procedures and processes implemented in the organisation to all employees affected by them.

In this regard, whenever a new rule is approved, an email will be sent to those members of the organisation affected by it, so that they are aware of its entry into force. Communication will be in simple language that is understandable to all employees.

If a rule is approved that affects business partners or third parties, the company will inform these third parties of its approval and how it affects their relationship with the organisation.

Communications will also be used to raise awareness of the importance of complying with *Corporate Compliance* rules, so that certain core rules, such as the Code of Ethics, can be communicated periodically to ensure that all members of the organisation are aware at all times of the guidelines they must follow and act accordingly.

6.2. TRAINING

Once the communication has been made, in the case of certain complex rules, a training session will be held on their content to explain to members of the organisation how they should be applied.

6.3. ACCESS

MASERGRUP, through its Intranet, provides all employees with access to the rules approved by the company.

Similarly, all members of the organisation can address their questions and concerns regarding *compliance* to both their department managers and the *Compliance Officer*, who are available to answer any questions so that all members are aware of, understand and are committed to complying with the law, internal regulations and the commitments voluntarily undertaken by the organisation.

6.4. DOCUMENTATION OF OPERATIONS AND CONTROLS. STORAGE AND FILING

The application of *compliance* controls generates documentation that must be filed, both for the effectiveness of the company's criminal risk management system and to provide evidence of the functioning of the specific control.

For this reason, the obligation to document and retain all operations, controls and other actions carried out by operational management and the *Compliance Officer* has been established.

7. COMMUNICATION OF OPERATIONS AND DISCIPLINARY REGIME

7.1. WHISTLEBLOWING CHANNEL ("SII")

All MASERGRUP employees and managers must report any breach of the law, internal regulations or voluntary commitments made by the organisation of which they reasonably suspect or are aware.

To this end, the company has made available to all its members an Internal Information System ("SII"), also known as the Integrity Channel, through which they may, in good faith and based on reasonable evidence, report any potential breach of the Criminal Risk Management System or internal corporate regulations.

INTERNAL REPORTING SYSTEM ("IRS")	
OBJECTIVE	**Report** inappropriate and irregular conduct
CHANNELS	Corporate website. **canalintegridad@masergrup.com**
RESPONSIBLE FOR THE SII	**Mr. Xavier Grau Beltran** *Compliance Officer*

Likewise, at the request of the communicator, a **face-to-face meeting** may be held with the SII Manager to explain or detail the facts of the communication. In this regard, if a communication of non-compliance is received and the informant fails to report it, the SII Manager shall be responsible for reporting it through the platform set up for this purpose. In such a case, verbal communications will be duly documented in accordance with the provisions of section 8 of the SII Policy.

Notwithstanding the above, any formal communication from a judicial body or public administration shall be considered a valid means of becoming aware of a breach.

The SII may be used by any person, whether a member of MASERGRUP or a third party outside the company, in particular suppliers, customers and business partners, regardless of whether they have already terminated their professional relationship with the company.

Likewise, communications may be made either **anonymously** or **identified** and will be treated and considered in the same manner.

All communications received that appear to be credible will be investigated with the necessary autonomy and independence and, in all cases, guaranteeing the rights of the person making the communication and of the persons to whom the facts communicated refer. The data will be processed in strict compliance with the legislation on personal data

protection, always ensuring that the identity of the persons making use of it will be treated with the utmost confidentiality and that there will be no reprisals against them.

If the breach is proven to be true, the offender will face disciplinary measures which, in accordance with the Workers' Statute and the applicable Collective Agreement, may lead to disciplinary dismissal.

To ensure the effective functioning of the SII, the company has approved the Protocol for the Management, Investigation and Resolution of Reports of Breaches ("**GIR Protocol**"), which regulates the use of the SII and the procedure to be followed in the subsequent investigation of incidents brought to the attention of the organisation.

MASERGRUP encourages all employees, managers and team leaders to act proactively and report any potential breaches. In addition to the above, the company's managers must commit to leading by example and being the highest exponents of the principles and values set out in the Code of Ethics.

7.2. PROHIBITION OF RETALIATION AND PROTECTIVE MEASURES FOR WHISTLEBLOWERS

Those who report any type of breach, as provided herein and in good faith, are **protected** against any type of retaliation, discrimination or penalisation because of the reports made. No measures shall be taken, either during or after the investigation, that could harm the whistleblower's professional career or lead to the termination of their employment. In addition, the company will punish any type of retaliation against whistleblowers acting in good faith.

The above prohibition of retaliation shall not prevent the adoption of appropriate disciplinary measures when the internal investigation determines that the report is false and that the whistleblower made it know it to be false and acting in bad faith.

In any case, retaliation shall be understood as any direct or indirect action or omission that takes place in a work context, is motivated by an internal or external report or by a public disclosure and causes or may cause unjustified harm to the whistleblower. By way of example, and without this being an exhaustive list, the following are considered retaliation:

(i) Suspension of the employment contract, dismissal or termination of the employment or statutory relationship, including non-renewal or early termination of a temporary employment contract after the probationary period has expired.

(ii) Early termination or cancellation of contracts for goods or services.

(iii) Imposition of any disciplinary measure, demotion or denial of promotion, and any other substantial change in working conditions.

(iv) Failure to convert a temporary employment contract into a permanent contract, where the worker had legitimate expectations that he or she would be offered permanent employment.

(v) Damages, including reputational damage, or economic losses, coercion, intimidation, harassment or ostracism.

(vi) Negative evaluation or references regarding work or professional performance.

(vii) Inclusion on blacklists or dissemination of information in a specific sector, which hinders or prevents access to employment or the contracting of works or services.

(viii) Refusal or cancellation of a licence or permit.

(ix) Denial of training.

(x) Discrimination, unfavourable or unfair treatment.

The measures set out in points (i) to (iv) above shall not be considered retaliation when carried out in the regular exercise of management powers under labour legislation or regulations governing the status of public employees, due to circumstances, facts or proven infringements, and unrelated to the submission of the report.

Likewise, in accordance with *Article 36 of the Whistleblower Protection Act*, it is hereby stated that any person whose rights have been violated as a result of their communication or disclosure, once the two-year period has elapsed, may request protection from the competent authority, which, in exceptional and justified cases, may extend the period of protection, after hearing the persons or bodies that may be affected. (the refusal of such an extension of the protection period must be justified).

Likewise, it is hereby stated that any acts intended to prevent or hinder the submission of communications and disclosures, as well as those that constitute retaliation or cause discrimination following their submission under the Whistleblower Protection Act, shall be null and void and shall give rise, where appropriate, disciplinary or liability measures, which may include the corresponding compensation for damages to the injured party.

MASERGRUP, recognising the aims of *Article 20 of the Whistleblowing Directive* and *Article 37 of the Whistleblower Protection Act*, will ensure that all its members have access, as appropriate, to the following support measures:

(i) Comprehensive and independent information and advice on the procedures and resources available to them in relation to regulatory compliance, protection against retaliation, and their rights as affected persons.

(ii) Effective assistance, essentially from the Internal Information System Manager, in the event of retaliation.

(iii) Legal assistance in any judicial or administrative proceedings that may arise as a result of their communications, whether national or cross-border, in the latter case in accordance with Community legislation.

(iv) Financial assistance and support measures in their capacity as whistleblowers, including psychological support after assessment of the circumstances arising from the submission of the report.

All of the above, in addition to any assistance to which the reporting person may be entitled under Law 1/1996 of 10 January on free legal aid for representation and defence in legal proceedings arising from the submission of the report or public disclosure.

Also with regard to reports, this Anti-Corruption Policy shall be made available to all MASERGRUP employees, as well as to all its business partners and third parties who, due to their relationship with the company, need to be aware of its content.

7.3. DISCIPLINARY REGIME

In accordance with the provisions of MASERGRUP's "**Disciplinary regime for breach of the Corporate Compliance System**", in order to ensure the effectiveness of the *Corporate Compliance* System*,* the punishable conduct indicated has been included in the company's Disciplinary Code, which shall apply to all MASERGRUP employees who fail to comply with their obligations in relation to the prevention of crimes and which may constitute a very serious offence in accordance with the provisions of Article 54 of the Workers' Statute.

8. PERIODIC VERIFICATION OF THE CRIMINAL RISK MANAGEMENT SYSTEM AND CONTINUOUS IMPROVEMENT

Both the entire criminal risk management system and the *compliance* controls that comprise it are continuously reviewed by MASERGRUP to identify weaknesses or areas for improvement. Once identified, the *Compliance Officer* will work to remedy or optimise them.

In any case, whenever a breach of the *Corporate Compliance* system is detected, MASERGRUP will react by taking whatever measures are deemed necessary to control and correct it, as well as to deal with any consequences that may arise. In this regard, the company:

1. Assess the need to take the necessary actions to eliminate the causes of the breach, with the aim of preventing it from happening again, by:
    a. Analysing the facts of which it is aware.
    b. Determining the causes of the breach.
    c. Investigating possible similar breaches that may also have occurred or may occur.
2. It will take all necessary actions to correct the non-compliance and prevent similar non-compliance in the future.
3. It will review all corrective actions it has taken to verify their effectiveness.
4. You will make any changes necessary to improve the *Corporate Compliance* system implemented.

This entire process will be duly documented.

In addition, the company's *Corporate Compliance* system will be reviewed whenever there are relevant regulatory or jurisprudential changes, changes in the structure or activity of the company, or for other reasons, which will be duly justified, as decided by the Sole Administrator or the *Compliance Officer* himself.

In any case, a comprehensive review of the system will be carried out every six months.

As part of the periodic reviews or those carried out due to non-compliance, regulatory or jurisprudential changes, changes in the organisation or the activity it carries out, or other duly justified reasons, the company will review the criminal risk analysis carried out, confirming that the criminal risks already detected continue to exist and analysing the possible emergence of new risks not previously considered.

Finally, the *Compliance Officer* will always act to lead the commitment to the company's values and reinforce the culture of compliance with the law and internal regulations.

9. PLANNING OF THE *CORPORATE COMPLIANCE* SYSTEM

9.1. ACTIONS TO ADDRESS RISKS AND OPPORTUNITIES

MASERGRUP's *Corporate Compliance* System has been planned in accordance with the issues referred to in section 4.1 and the requirements referred to in section 4.2 of *Standards UNE 19601* and *UNE ISO 37001*, determining the risks and opportunities that need to be addressed to:

(i) Reasonably ensure that the *Corporate Compliance* System can achieve compliance objectives, establishing itself as an organisational and management model that includes appropriate monitoring and control measures to prevent crimes or significantly reduce their occurrence.

(ii) Prevent or reduce undesirable effects related to the System's Policies and objectives.

(iii) Monitor its effectiveness and achieve continuous improvement.

9.2. OBJECTIVES OF THE *CORPORATE COMPLIANCE* SYSTEM AND PLANNING TO ACHIEVE THEM

MASERGRUP has established the following objectives for the *Corporate Compliance* System for the relevant functions and levels:

(i) To inform MASERGRUP employees about the *Corporate Compliance* System and the organisation's policies governing it.

(ii) Maintain effective controls to prevent irregular conduct or conduct that contravenes the regulations of the *Corporate Compliance* System, reviewing them periodically and implementing actions to reinforce them or including additional ones that strengthen the System.

(iii) Respond promptly to any case reported through the SII, applying the methodologies of the *Corporate Compliance* System, ensuring the correct handling of cases and the application of sanctions where appropriate.

(iv) Report to the joint administrator in an annual report on the functioning of the System and the continuous improvement measures implemented.

The above objectives are in turn:

(i) Consistent with the provisions of the policies and procedures that make up MASERGRUP's *Corporate Compliance* System, as they have been established in accordance with the context of the organisation, the requirements of the interested parties and the results obtained.

(ii) They are measurable according to the KPIs specified in the "KPIs" section, which provide information and measure the effectiveness of the actions implemented to achieve the objectives.

(iii) They consider the factors applicable in section 4.1 of standards UNE 19601 and UNE ISO 37001 and determine the risks identified in section 4.5 of the same standards.

(iv) They are achievable.

(v) They are monitored.

(vi) They have been communicated in accordance with section 7.5 of Standard UNE 19601 and 7.4 of UNE ISO 37001.

(vii) They are updated as appropriate.

Furthermore, MASERGRUP's business partners are informed of the policies governing the company, which are available on the company's website.

The team responsible for the *Corporate Compliance* System periodically carries out the necessary planning to achieve the objectives of the System, in which it determines:

(i) What is to be done.

(ii) The resources that will be required.

(iii) Who will be responsible.

(iv) When the objectives will be achieved.

(v) How the results will be evaluated and reported.

(vi) Who will be responsible for imposing sanctions or penalties.

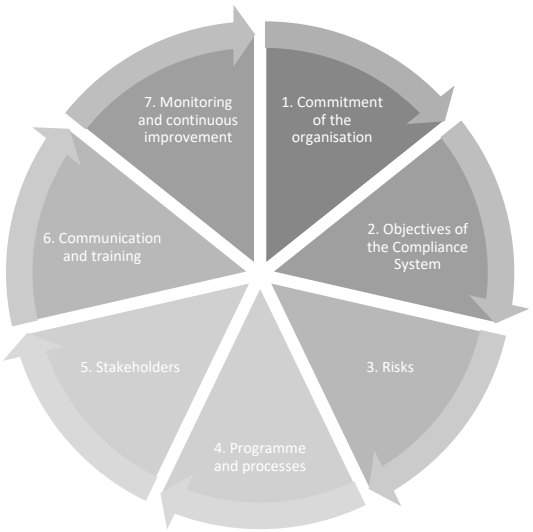
9.3. KPI INDICATORS

Compliance management indicators or *Key Performance Indicators* (KPIs) are performance metrics that demonstrate the effectiveness of the programme and visualise patterns and trends, as well as measure progress towards specific goals and objectives.

In this way, KPIs measure the capacity of MASERGRUP's *Compliance* System to keep the organisation in line with both internal and external policies, as well as with government regulations.

The following KPIs form the basis of MASERGRUP's *Compliance* Management System (CMS) or *Corporate Compliance* System, in accordance with UNE 19601 and UNE ISO 37301 standards, which require the use of compliance management indicators to measure the effectiveness of the *Corporate Compliance* System and verify the effective implementation of *compliance* controls, as well as the actual progress towards the achievement of the company's compliance objectives.

MASERGRUP has considered the following KPIs to measure the level of compliance with the company's *Compliance* Management System:



(i) **Organisational commitment:** first, an assessment will be made of whether the compliance culture and values of the company reflected in the Code of Ethics are known and respected by all its members.

(ii) **Objectives of the *Corporate Compliance* system:** an assessment will be made of whether the action plans and objectives set by the *Compliance Officer* have been adequate and fulfilled.

(iii) **Identification and management of *compliance* risks**: consideration will be given to whether the company has carried out or updated an assessment of the criminal risks affecting it during the current year.

(iv) **MASERGRUP programme and processes**: the level of compliance with the implementing regulations implemented by the company will be considered, and whether there has been any regulatory breach and whether it has been dealt with appropriately (by investigating, imposing sanctions on those involved, taking measures to mitigate its effects, etc.).

(v) **Global *compliance* organisation**: consideration will be given to whether the *Compliance Officer* is truly independent from the joint administrator and whether their functions are properly defined.

(vi) **Communication and training:** an assessment will be made of whether MASERGRUP has provided regular communication and training to its members on *corporate compliance* matters.

(vii) **Monitoring and continuous improvement** of the *Compliance* Management System: an assessment will be made of whether the company adequately monitors and implements appropriate improvement measures in its *Corporate Compliance* System.

10. SUPPORT

10.1. RESOURCES

MASERGRUP has the necessary human resources for the establishment, implementation, maintenance and continuous improvement of the *Compliance* Management System, which is the responsibility of the company's *Compliance Officer*.

MASERGRUP also has various physical resources to ensure the proper functioning of the Compliance Management System.

On the one hand, the team responsible for the *Compliance* Management System has a physical space, as well as the necessary amenities and resources to operate.

On the other hand, about physical security, MASERGRUP has surveillance strategies in place, including video surveillance cameras inside the offices and the workshop to ensure the security of the activities carried out on the premises. Likewise, the areas within the premises are strategically distributed to safeguard sensitive documentation.

Finally, MASERGRUP has sufficient financial resources to ensure that the *Compliance* Management System functions effectively.

10.2. COMPETENCE

In accordance with point 7.3 of the *UNE 19601 standard*, regarding competence, MASERGRUP:

(i) Determines the necessary competence of persons who, under its control, perform work that affects the performance of *the Compliance* System. To this end, each year, the *Compliance Officer* defines a training plan, as well as the areas to be covered by each training course, to generate and maintain the appropriate competences.

(ii) Through these training courses, MASERGRUP ensures that these individuals are competent. The courses are delivered in person, online and, on occasion, in an e-learning format.

(iii) Take action to acquire and maintain the necessary skills and evaluate the effectiveness of the actions taken.

(iv) Keep appropriate documented information as evidence of competence.

10.3. HIRING PROCESS

Regarding personnel hired by MASERGRUP, the organisation implements various procedures:

(i) The terms and conditions of employment require staff to comply with the *Compliance* Management System (CMS) and grant the organisation the right to apply the disciplinary measures provided for in the event of non-compliance with

the CMS. MASERGRUP's job offers clearly state that the organisation has a *Compliance* Management System and that it is important that the profile of candidates for the vacancy in question complies with its principles. Once selected, and in the respective offer, the person will be obliged to comply with the SGC, including the applicable policies.

(ii) Once the employment relationship has begun, employees are provided with access to all the policies and procedures that make up MASERGRUP's *Compliance* Management System via the company's intranet, where they can access, view and download a copy of any of them. During the welcome process, all employees are required to undergo *compliance* training, which includes a brief description of the company's policies, including the SGC. This is evidenced by the attendance list and the content of the presentation given to new hires.

(iii) MASERGRUP has procedures in place that allow it to take appropriate disciplinary action against personnel who violate or fail to comply with company policies or the Compliance Management System.

MASERGRUP also has a disciplinary regime for breaches of the QMS, which aims to establish procedures that allow the organisation to take appropriate disciplinary action against individuals who may violate the System's policies and procedures.

(iv) Staff shall not suffer reprisals, discrimination or disciplinary measures for (i) refusing to participate in, or rejecting, any activity which they reasonably consider involving a criminal risk, if they have previously reported this to the SII; (ii) or for reporting in good faith through the SII.

10.1. DUE DILIGENCE

MASERGRUP, in accordance with section 6.2 of *Standard UNE 19601*, will carry out a Due Diligence procedure with respect to activities in which criminal risks that must be prevented may arise and where the risk is higher than low in relation to:

(i) Transactions, projects or specific activities.

(ii) Current or planned business relationships with certain business partners (*Business Partner Due Diligence*), such as:

a. Business partners with the ability to act on behalf of MASERGRUP that pose a greater risk to it than suppliers of goods or services from the perspective of potential criminal liability.

b. The degree of influence that MASERGRUP has over its business partners may also affect the scope of the investigations.

(iii) Categories of personnel in specific categories to verify that the position is appropriate and that it is reasonable to believe that they will fully understand this Policy and comply with it.

11. CHANNEL FOR QUESTIONS AND/OR SUGGESTIONS

Remember that if you have any **questions or suggestions** regarding the interpretation or application of the content of this Policy, the company's Corporate Compliance System, or any other matter related to regulatory compliance, you should immediately contact the *Compliance Officer* by sending an email to the following address:

compliance@masergrup.com

However, the **reporting** or communication of inappropriate, irregular, or un y conduct that may violate the content of this Policy must be reported through the **SII** or **Integrity Channel** set up for this purpose, as provided for in section 7.1 of this Policy.

COMMUNICATION CHANNELS	
QUESTIONS AND SUGGESTIONS FROM *CORPORATE COMPLIANCE*	**Enquiry Channel** compliance@masergrup.com
REPORT INAPPROPRIATE AND IRREGULAR CONDUCT	**Integrity Channel** Corporate website canalintegridad@masergrup.com

APPENDIX I. APPROVAL AND AMENDMENTS

APPROVAL AND AMENDMENTS	
VERSION NUMBER	2
APPROVED BY	Sole Administrator
RESPONSIBLE	*Compliance Officer*
DATE OF INITIAL APPROVAL	March 2025
DATE OF FIRST AMENDMENT	July 2025