TECHNICAL INSTRUCTION
CRIMINAL PREVENTION PROTOCOL
(Legal Compliance)

LIST OF MODIFICATIONS/APPROVALS

List of modifications

Edition	Date	Modification
1.0	07/01/21	Creation
1.1	06/09/21	Point 5.3 and the external company

Approvals

E	R	A	Position	Name
	X	X	Quality	Víctor Orero
X			Occupational Risk Prevention	Eli Colomer
	X		Tactik	Agustín Ruiz

E: Edited R: Revised A: Approved

1. INTRODUCTION

1.1. Concept and evolution

Legislative evolution creates a need for the company to adapt to change and adopt new practices and policies accordingly.

The Corporate Compliance concept, as well as the figure of the Compliance Officer, were imported from the Anglo-Saxon system and started to take off in Spain with the reform of the Criminal Code (approved through Organic Law 5/2010, of 22 June, amending Organic Law 10/1995, of 23 November, on the Criminal Code, and which came into force on 23 December 2010). It took off even more so with the 2015 reform (Law 1/2015, of 31 March, amending Organic Law 10/1995, of 23 November, on the Criminal Code), which extended the regulation of the criminal liability of legal persons (Article 31 bis), thus making legal persons susceptible to committing criminal offences. This led to the implementation of criminal prevention protocols to try to prevent criminal risks and even avoid incurring criminal liability for the commission of such offences, exempting or extenuating, where appropriate, the possible criminal liability that would therefore be transferred to the legal person.

In fact, the recent reform of the Criminal Code in 2015 presents us with the organisational and management models that include the ideal vigilance and control measures to prevent offences. This enables companies to self-regulate and implement criminal prevention mechanisms adjusted to their structure and operation.

Implementing these protocols in a company implies being covered and informed about all aspects related to criminal law.

1.2. Structure and activity of ASINTEL

ASINTEL was founded in 1988 as a telecommunications consultancy and engineering company to provide these services to FECSA – ENDESA and GAS NATURAL.

It is currently located in Sant Cugat del Vallès, in a 180-m^2 establishment with offices, a warehouse, a workshop and a laboratory. It also has a delegation in L'Hospitalet de l'Infant (Tarragona).

It has its own fleet of four-wheel-drive vehicles, vans and cars. It owns the software and the electronic and measuring equipment it needs to perform the work commissioned with guarantees.

The company focuses its activity on the telecommunications sector in both cable systems (optical and electrical) and wireless systems (PMR, DMR, TETRA, WiFi, Wimax, radio-links, etc.), providing a global communications service.

Currently, and in general, we perform the following jobs:

- Consultancy, engineering, and design of infrastructures and communications systems.
- Supply of equipment and installation and commissioning of communications systems.
- Global turnkey projects, from the first consultation and site management to the delivery of the completed and documented project.
- Coverage, field measurements, feasibility, and audits of communications systems.
- 24/7 maintenance of different equipment, communication systems (cable or radio) and infrastructures.
- Official Telecommunications Operator [National Commission for Markets and Competition (CNMC)] that provides data, internet and mobile communication services.

Therefore, the scope of the ASINTEL, S.L. Management System is defined as: "Global communication services. Engineering and maintenance of communications systems", both at its centres in:

Baixada de l'Alba, 16 - 08172 – Sant Cugat del Vallès – Barcelona

Hospitalet de l'Infant - Tarragona

As well as at the sites where it carries out work arising from the activities that fall within the system's scope.

2. SUBJECT MATTER, SCOPE OF APPLICATION AND METHODOLOGY

2.1. Subject matter of the Protocol

This Protocol aims to implement an appropriate system for the development of good practices and a risk prevention process within ASINTEL and, specifically, in those cases of commission of offences referred to in Article 31 bis 1 of the Criminal Code:

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 make decisions on behalf of the latter or have organisational and control powers within it.*

b) *For offences committed in the course of their business and on their behalf and for their direct or indirect benefit, by those who, being subject to the authority of the natural persons referred to in the preceding paragraph, may have committed the acts through a serious non-compliance with their duties of supervision, vigilance and control of their activity, given the specific circumstances of the case.*

Therefore, this Protocol works as a mechanism that can exercise control over the actions of ASINTEL's members, in such a way that, if due diligence is proven, the legal person will not be liable for the offences committed by such members, and/or its liability would be extenuated if effective control measures have been established to prevent, detect and report offences that could be committed using ASINTEL's means or under ASINTEL's cover. The objectives of this Protocol are as follows:

- To prevent the commission of any of the offences listed below by its legal representatives, Managers or employees through the application of the Protocol.
- To ensure the effectiveness of control standards and procedures in order to minimise risks and illegal behaviour.
- To inform all employed staff of the consequences and sanctions that ASINTEL may impose if they commit the listed offences.
- To make clearly and categorically known that ASINTEL condemns any conduct that contravenes the Law and that such conduct constitutes a breach of internal policies and procedures.
- To prove that ASINTEL has exercised appropriate control over the development of its business activities, therefore complying with the requirements of the Criminal Code in force.
- To inform and make all ASINTEL staff aware of possible conduct that could be considered criminal, conveying the message that strict compliance with the policies and procedures established in this Protocol will prevent the possible commission of offences.
- To implement an optimal channel that can resolve and process all situations in which ASINTEL members may see a breach of the regulations in force.

- To help all ASINTEL's employed staff to comply with the applicable rules of this Protocol by providing them with a clear statement of policies and procedures.
- And finally, to cover and support the establishment of effective measures for a better detection and control of offences committed within legal persons.

For all of the above, not only does this Protocol intend to avoid criminal sanctions against ASINTEL, but also to promote a culture of business ethics and compliance, expressing the firm will of ASINTEL's Management to comply and enforce compliance with the Law whilst conveying a corporate commitment that truly discourages criminal conduct. Such a commitment will be mandatory for all Directors, Managers and employees.

2.2. Scope of application

This Protocol applies to ASINTEL as a whole. Its observance and application will be mandatory for both employees and managers of legal persons. Similarly, those employees who carry out commercial activities for companies linked by a commercial relation, that is, under any form of collaboration, will be affected, insofar as they take part in the production processes with criminal risks included in the criminal risks matrix that we will see further on.

2.3. Methodology

To draw up this Protocol, we have followed a method to customise the criminal risks that may arise within ASINTEL through an approach to the normal and usual operation of the companies that comprise it. We analysed the usual conduct, the procedures established for the performance of their daily activities and the protocols they follow in order to comply with their internal regulations and the legally established rules in the different fields that affect ASINTEL.

Once the existing processes were determined, we identified the criminal risks existing in the legal persons according to the activities each of them carries out and classified them according to their impact and likelihood, thus obtaining a table of risks adapted to ASINTEL.

Following this, we drew up a disciplinary system that sets out how the company should act in situations of non-compliance with the prevention systems established in this Protocol, as well as the corrective measures that may be implemented in the event of the commission of an offence by any person that is part of ASINTEL or in the event of non-compliance with the obligations stipulated in terms of compliance.

Likewise, we have set up an ethical or whistleblowing channel that will serve as a means of communication to allow legal persons to be informed of any potential breaches of current regulations that may occur and that affect them in any way. Consequently, appropriate checks can be initiated, in addition to the appropriate measures been taken. ASINTEL has also been provided with a supervisory and control body that will also serve as a body that investigates, classifies, files and processes complaints or communications received.

Lastly, we can expect mechanisms for the updating and supervision of the prevention model.

3. CRIMINAL RISK ANALYSIS

3.1. Criminal risk assessment and criminal risk table

The table of criminal risks that apply to ASINTEL is set out below. Regarding the types of risks that can be attributed to legal persons, not all of them can be included within the scope of the specific activities carried out directly and indirectly by ASINTEL. Therefore, the following is a list of those that should reasonably be prevented, even if they are far from being considered likely, and always under the assumption that total prevention is unattainable.

The table of risks is structured as follows:

i. The article of the Criminal Code in force that corresponds to each offence.
ii. The criminal conduct constituting an offence, that is, the conduct included in the article.
iii. The likelihood of the risk appearing in ASINTEL using a scale with three different values. The lowest level, "Unlikely", corresponds to risks that are unlikely to appear within the company. The intermediate level, "Possible", is for those risk situations that, without being present in ASINTEL's day-to-day business, *do* exist on a regular basis and relatively frequently. Lastly, the highest level, "Very likely", is for risks that are present in ASINTEL's day-to-day business, such that the possibility and likelihood of their commission makes them worthy of special attention.
iv. The impact as in the severity of the consequences that ASINTEL may face for the commission of the criminal offences described above in terms of the penalty that may be imposed. To this end, three severity levels have been established. The lowest level, "Low", is for those offences which, if they were to

occur, would only lead to penalties of a financial nature. The intermediate level, "High", is for those cases in which the consequences of the commission of the offence, without entailing penalties reserved for those classified as severe, may be aggravated by the extension of its consequences beyond the criminal scope. Lastly, the highest level, "Severe", is reserved for conduct which, if it were to occur, would have such consequences that it could possibly lead to the dissolution or suspension of the company's activities.

ASINTEL CRIMINAL RISK TABLE

LIKELIHOOD LEVEL	CODE	SEVERITY LEVEL	CODE	IMPACT LEVEL	CODE
VERY LIKELY	VL	HIGH	HI	SEVERE	S
POSSIBLE	P	LOW	LO	HIGH	H
UNLIKELY	UN			LOW	L

CRIMINAL CONDUCT (TYPE OF OFFENCE)	LIKELIHOOD	SEVERITY	IMPACT
1.- Discovery and disclosure of secrets and breach of the right to privacy	UN	LO	L
2.- Swindling through deceit	UN	LO	L
3.- Swindling through computer manipulation or a similar device	UN	LO	L
4.- Swindling by manufacturing, introducing or possessing specific software to commit swindles	UN	LO	L
5.- Swindling through the illegal use of credit or debit cards, or travellers' cheques, or the details that appear on any of them	UN	LO	L
6.- Carrying out acts of disposal without having a valid right to do so	UN	LO	L
7.- Carrying out acts of disposal with the concealing of charges or encumbrances	UN	LO	L
8.- Fraudulent concealment or disposal of assets	UN	LO	L
9.- Frustration of foreclosure: hindering the effectiveness of legal proceedings brought by the creditor through acts of disposal of assets	UN	LO	L

CRIMINAL CONDUCT (TYPE OF OFFENCE)	LIKELIHOOD	SEVERITY	IMPACT
10.- Frustration of foreclosure: activities aimed at attempting to circumvent civil liability arising from the commission of an offence	UN	LO	L
11.- Providing an incomplete or falsified list of assets in enforcement proceedings	UN	LO	L
12.- Using seized goods that have been placed in storage without proper authorisation	UN	LO	L
13.- Punishable insolvency in all its forms	UN	LO	L
14.- Computer damage: erasing, damaging, deteriorating, altering, suppressing or rendering inaccessible other people's computer data, computer programmes or electronic documents	UN	LO	L
15.- Obtaining economic gain from the use of works protected by copyright without proper authorisation	UN	LO	L
16.- Intentionally using a patent or utility model without proper authorisation for commercial purposes	UN	LO	L
17.- Offering the above patents or utility models for the same purposes to third parties	UN	LO	L

CRIMINAL CONDUCT (TYPE OF OFFENCE)	LIKELIHOOD	SEVERITY	IMPACT
18.- Manufacturing, marketing, distributing or importing counterfeit or imitation goods	UN	LO	L
19.- Fraudulent use of the designation of origin	UN	LO	L
20.- Theft of corporate information	UN	LO	L
21.- Disclosing information or business secrets that one was obliged to keep	UN	LO	L
22.- Using false or misleading advertising that causes or is likely to cause harm	UN	LO	L
23.- Manipulation of computerised accounting or measuring equipment used for invoicing purposes	UN	LO	L
24.- Using deceit or violence to alter prices	UN	LO	L
25.- Disseminating false information to alter stock market prices	UN	LO	L
26.- Corruption in business: obtaining benefit to favour someone else in a business relationship	UN	LO	L
27.- Corruption in business: bribing another person to obtain an unduly favour in a business relationship	UN	LO	L

CRIMINAL CONDUCT (TYPE OF OFFENCE)	LIKELIHOOD	SEVERITY	IMPACT
28.- Corrupting or attempting to corrupt civil servants regarding the conduct of international business activities	UN	LO	L
29.- Receiving stolen goods: acquiring, possessing, using, converting or conveying assets knowing they originate from a criminal activity	UN	LO	L
31.- Fraud against the European Union exceeding €50,000	UN	LO	L
33.- Inducing into error to obtain social benefits, or unduly extend benefits, for oneself or a third party	UN	LO	L
34.- Accessing Public Administration funds by falsifying data	UN	LO	L
35.- Using public funds obtained for purposes other than those for which they were granted	UN	LO	L
36.- Not keeping the mandatory accounts while under direct tax assessment	UN	LO	L
40.- Causing or producing emissions or discharges that damage or may cause damage to the air, water, soil, flora or fauna	UN	LO	L
41.- Causing or producing noises, vibrations, injections or deposits that damage or may cause damage to the air, water, soil, flora or fauna	UN	LO	L

CRIMINAL CONDUCT (TYPE OF OFFENCE)	LIKELIHOOD	SEVERITY	IMPACT
42.- Exploiting installations for hazardous activities without respecting the regulations in force	UN	LO	L
43.- Manufacturing, handling, transporting, holding or commercialising explosives, flammable, toxic or corrosive substances, in breach of the corresponding regulations, and endangering people or the environment	UN	LO	L
44.- Counterfeiting of medical devices, medicines or active substances	UN	LO	L
45.- Producing false documents, labelling, etc., for the above items	UN	LO	L
46.- Bribery [*cohecho*]: promoting the bribery of a civil servant so that they carry out an act that is contrary to those they ought to perform, or delay or fail to perform an act which they ought to perform	UN	LO	L
47.- Bribery [*cohecho*]: to accept the request of a civil servant to carry out the conduct detailed in the previous paragraph	UN	LO	L
48.- Influencing a civil servant by taking advantage of a personal relation to obtain a benefit	UN	LO	L

Other conduct to be controlled: sexual harassment, harassment in the workplace or mobbing.

3.2. Existing control mechanisms

1.- Natural resources and the environment: there is strict compliance with environmental regulations in addition to a thorough control of stored materials and equipment, which are inventoried periodically at ASINTEL.

2.- Models for the prevention of legal risks in the workplace: specifically, those concerning regulatory compliance by ASINTEL's own employees and managers, and their internal actions within the companies (prevention of harassment, use of technological means at work, insider information, etc.).

The Prevention Plan can be found in Annexe I.

There is a Technical Instruction, namely IT229 "Harassment Prevention Protocol", which describes measures to prevent harassment inside the company.

Additionally, Emergency Action Plans have been included. These aim to facilitate communication, evacuation and immediate intervention in the event of an emergency situation (Annexes V and VI).

The scope of application extends to all ASINTEL workplaces, whether permanent or temporary, and to all their employees.

Likewise, a Psychosocial Factors Assessment was carried out to identify and measure psychosocial working conditions that may pose a risk to the health and well-being of ASINTEL employees. Such assessment was presented as an instrument to provide the correct planning of preventive actions aimed at protecting the health of employees in compliance with the Law on Prevention of Occupational Risks [*Ley de Prevención de Riesgos Laborales*].

This way, these "codes of conduct" or "good practices" have been implemented to regulate behaviour in the company's workplaces, as well as global standards of responsible behaviour.

Furthermore, there is strict compliance with the regulations and coordination of the company's activities, all employees have the required safety and Occupational Risk prevention measures and regular medical check-ups are carried out.

4. PROTOCOL SUPERVISION AND DISSEMINATION

4.1. Protocol supervision and control

The continuous supervision of the Protocol is deemed necessary to ensure its proper functioning. As part of this continuous supervision, establishing two new bodies that will enable the Protocol to function effectively is essential:

Investigation and control body

The creation of a regulatory compliance control body is planned for ASINTEL. Such body will be made up of the Management Officer, the Environmental Officer and the Occupational Risk Prevention Officer, and will be able to carry out the necessary tasks of the plan's control body (updating and supervision), as well as the investigation of potential communications and/or complaints received through the ethical (whistleblowing) channel.

This work is essential to provide ASINTEL's decision-making body with reliable and accurate information that allows it to make decisions in accordance with the Law, and that are, in all aspects, in the best interest of ASINTEL.

Investigation work shall end with a report that includes, in any case and at least, the following information:

- Receipt of communications or complaints.
- Descriptive information on complaints, dates when they were filed and main milestones.
- Emergency measures carried out, the reasoning behind them and their effects.
- Proposals for action and resolution.

Feedback/decision-making body

This body will be in charge of the decision-making involving feedback of any kind regarding the potential materialisation of a criminal risk in any of ASINTEL's activities.

The body in charge of feedback will be a single person, in this case Mr Víctor Orero, and will be the same for the whole of ASINTEL. In its decision-making, it may seek support from any internal or external body or adviser, as well as from the investigating body.

We consider that it is important that there is a disassociation between the body in charge of investigating potential breaches and the person in charge of resolution and decision-making for the sake of reliability of the system, which is

based on objectivity and transparency concerning both the investigation and the resolution of communications and complaints.

4.2. Duties of the Compliance Officer

Supervision of the functioning of and compliance with this Protocol has been entrusted to its Compliance Officer, in particular to the persons mentioned in section 5.5, who shall have the following duties:

1. Duly control its implementation.
2. Follow-up and verify its implementation through specific activities aimed at monitoring continuous improvement of behaviours.
3. Ensure that they are complied with, updated and modified.
4. It will act as a channel for complaints, it will convey them accordingly, direct investigations into the possible commission of allegedly criminal conduct and propose the appropriate sanctions to the competent body of the Company.

4.3. Dissemination and updating of the Protocol

This Protocol will be available on ASINTEL's website so that employees and third parties who have a relationship with the companies can learn about ASINTEL's commitment to crime prevention within these companies and report, through the channel enabled to this end, the possible commission of offences or conduct that contravenes current regulations inside the company.

As for its updating, given that a prevention Protocol such as this one is a dynamic management system, it will be reviewed periodically every year. This review and updating task will be the responsibility of the regulatory compliance investigation and control body.

In any case, the Protocol review tasks will be called for if and when the following circumstances arise:

- Modification of the legal regulations governing the operation of ASINTEL or its business or activity sectors, as well as any relevant change in ASINTEL's control structure.
- Legal amendments that make its modification advisable or mandatory.

- When unexpected or relevant breaches of its provisions become apparent or when the risks of criminal conduct are reassessed, by updating the table of risks.

Subsequent reviews, modifications and updates shall be made by means of an Annexe to this Protocol.

5. ETHICAL (WHISTLEBLOWING) CHANNEL. APPOINTMENT OF THE COMPLIANCE OFFICER

5.1. Purpose

In order to provide a basis for this Protocol, an ethical (whistleblowing) channel must be created. Such channel will operate as ASINTEL's organisational structure and enable the response model to fulfil its objectives, since it will provide the necessary information on the potential commission of an offence or materialisation of a risk.

This channel provides ASINTEL employees and third parties with a medium to report any possible compliance breaches. It is available 24 hours a day and is managed solely by an independent expert external to ASINTEL. This independent expert will forward communications and complaints to the investigation and control body, allowing the complainant (whistleblower) to provide information in such a way that they are protected. Communications and complaints will be recorded and subsequently forwarded and analysed by the investigation and control body to determine whether there are grounds for non-compliance that require further action or investigation.

This independent external expert – in charge of receiving communications and complaints through the ethical (whistleblowing) channel related to non-compliance with this Protocol and breaches of compliance that may have taken place – will be the entity TACTIK.

Additionally, personal complaints may be submitted and any circumstance that may involve a breach of the Criminal Code may be reported.

It should be noted that confidentiality is the cornerstone of this ethical (whistleblowing) channel. This does not necessarily imply anonymity, since these communications or complaints are merely a mechanism to initiate an investigation to verify the facts reported, and the identity of the complainant (whistleblower) guarantees the accuracy and integrity of the information contained in the Complaint Forms and the Investigation Reports attached as Annexes VII and VIII.

5.2. Reporting breaches

Through this ethical (whistleblowing) channel, any person may make suggestions, claims or complaints regarding non-compliance with the internal codes of all ASINTEL workplaces and non-compliance with regulations, which will only be received by TACTIK (the external company). In order to be admitted and properly processed, the communications or complaints must necessarily include the following information, which will be included in the Complaint Form:

- Name and surnames of the complainant (whistleblower).
- A brief statement of the facts or grounds supporting the communication or complaint.
- Date/s and place/s.
- Possible witness/es.
- Signature of the complainant (whistleblower) and date of the complaint.

As stated above, both the EXTERNAL COMPANY and the control body will guarantee the confidentiality of the complainant (whistleblower), until the appropriate time, unless such information is requested by the competent authority, whether judicial or administrative. In this case, the workplace/s in which the offence was committed must provide such information to the requesting body.

5.3. Processing of complaints

The communication or complaint will be sent to the EXTERNAL COMPANY, either through the corresponding Complaint Form or via the following e-mail address:

agustin@tactik.es

Upon receipt of the communication or complaint, the EXTERNAL COMPANY will forward it to the appropriate designated Compliance Officer, who will start the appropriate inquiries. If the communication or complaint concerns any of the persons forming part of the investigation body, said person must be replaced immediately.

5.4. Investigation procedure

The procedure is divided into the following stages:

a) Receipt and registration of complaints

As indicated in the previous section, any person may report offences or breaches of this Protocol of which they are aware suing the e-mail address indicated above or by submitting the Complaint Form.

b) Analysis of the admissibility of the alleged facts

Once the complaint has been received through any of the aforementioned channels, TACTIK (the external company) must forward it to ASINTEL's Compliance Officer, who will carry out a preliminary assessment of background information. To this end, they may interact with the complainant (whistleblower) and/or possible witnesses to give an appropriate and timely course to the investigation. Subsequently, an admissibility analysis must be carried out based on the background information gathered to determine whether the alleged facts should be investigated. Based on the analysis, one of the following procedures will be adopted as appropriate:

- If the submission only related to a complaint about operational or management aspects of any of ASINTEL's workplaces or any other statement that does not constitute a breach of this Protocol or an offence and therefore does not require an internal investigation, it shall be immediately referred to the corresponding internal area of the company for the provision of feedback and/or the adoption of the relevant measures. In such cases, the Compliance Officer may issue a report with best practice recommendations to the internal area responsible for the matter.
- In the event of complaints about facts that constitute a breach of this Protocol or an offence, an investigation shall be opened and conducted in accordance with the procedure set out herein.

The statement of admissibility of the complaint must be made within a maximum of 10 days after it is brought to the attention of the Compliance Officer.

c) Investigation of the alleged facts

Investigations into possible offences and Protocol breaches will be conducted by the Compliance Officer, who shall issue the Investigation Report within 20 days from the date of the complaint or communication.

During the investigation, the Compliance Officer may undertake all activities and arrangements necessary for the investigation, such as interviewing persons who are potentially involved or third parties who may have information on the facts, obtaining expert opinions or reports, etc. If needed, the Compliance Officer may engage the services of external advisers or specialists to support the investigation.

d) Investigation report

The Compliance Officer will draw up an Investigation Report that must include the background information of the case, the followed procedures, and the conclusions and recommendations, if any. The Investigation Report will be submitted to the Officer of the decision-making body.

e) Assessment for the implementation of measures

Once the Officer of the decision-making body has received the report, it must provide a response on the appropriate actions to be taken, such as the initiation of civil or criminal actions; or the adoption of work-related sanctions or disciplinary measures; or the application of corrective measures to the procedures or control measures in which flaws have been detected.

f) Resolution and notification

Once the resolution of the case has been issued, the Compliance Officer or the Officer of the decision-making body shall communicate the result of the investigation and the actions to be taken in this regard to the reported party by any reliable means, within 5 days, briefly and in general terms.

All deadlines indicated in this procedure will be in working days. Saturdays, Sundays and bank holidays will be understood as non-working days.

This procedure shall always be controlled by the Officer of the decision-making body.

5.5. Appointment of the Compliance Officer

The Compliance Officer will be chosen at the discretion of ASINTEL's management body, which, on the date of entry into force of this Protocol, will be the Management Officer, the Environmental Officer and the Occupational Risk Prevention Officer in representation of ASINTEL. This position shall have an indefinite term unless they are revoked by decision of the company's management body.

5.6. Revocation of the position of Compliance Officer

The Compliance Officer shall remain in office as long as they perform their duties diligently and following the provisions of this Protocol. This will be assessed annually by the management body.

5.7. Data protection

ASINTEL always guarantees the confidentiality of the complainant (whistleblower) and compliance with the rules on Personal Data Protection, in relation to the General Data Protection Regulation of the European Union 2016/976.

To this end, the communications or complaints made will generate a file that will be recorded, and all persons involved in possible investigation processes must maintain due confidentiality of the data and information to which they have had access until it is deemed appropriate, unless such information is required by the competent authority, whether judicial or administrative. In this case, the workplace/s in which the offence was committed must provide such information to the requesting body and may be sanctioned in the event of non-compliance.

6. DISCIPLINARY SYSTEM IN CASE OF NON-COMPLIANCE

If a legally prosecutable offence is found to have existed in ASINTEL, the relevant management body shall report it to the authorities.

The commission of the alleged offence legitimises ASINTEL to take disciplinary measures against someone, as appropriate, including dismissal, always applying the provisions of the General Workers' Statute, the Collective Bargaining Agreement or the signed Employment Contract.

Failure to report a breach, when known, may also be subject to disciplinary action.

If this occurs, the following sanctions are foreseen depending on the severity of the non-compliance or offence:

1. For the most serious breaches, which must necessarily constitute an offence, and for breaches of the specific duty to inform the control body of any non-compliances that may have been detected, the employee under investigation may be suspended from work as a precautionary measure with paid leave whilst the internal investigation file is being processed, in

order not to hinder the company's or the Compliance Officer's investigation work when it comes to gathering evidence or proof of the potential breach; dismissal may even be agreed. All of the above is at the discretion of the Officer of the decision-making body, depending on the severity of the matter and always in accordance with the applicable regulations.

2. For less serious breaches, the offender may be given a warning or a work-related disciplinary sanction. All of the above is at the discretion of the Officer of the decision-making body, depending on the severity of the matter and always in accordance with the applicable regulations.

These actions, among others, will ultimately constitute telling evidence of ASINTEL's commitment to regulatory compliance and crime prevention.

7. ENTRY INTO FORCE

This Criminal Prevention Protocol (Compliance Programme) shall enter into force on the same day of the date of its signature, that is, on 2022/09/06.

ANNEXES

ANNEXE I: Occupational Risk Prevention Plan - ASINTEL.

ANNEXE II: Risk Assessment Report - ASINTEL.

ANNEXES III and IV: Preventive Action Planning - ASINTEL.

ANNEXES V and VI: Emergency Action Plans - ASINTEL.

ANNEXE VII: Complaint Forms - ASINTEL.

ANNEXE VIII: Investigation Report Template - ASINTEL.