


PT1.1_1

**ACTION PROTOCOL FOR THE PURPOSES OF CRIME
CONTROL AND PREVENTION AND ANTI-FRAUD OF
SUARDIAZ GROUP**

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edition 03
		27/11/2023

REGISTER OF CHANGES

Edition	Date	Section	Page	Description of the change
01	10/12/2018			Initial Edition
02	19/12/2022			Ratification of Initial Edition
03	27/11/2023			Ratification of Initial Edition and incorporation of the Internal Information System Regulation

LIST OF INTERNAL DISTRIBUTION

Personnel/Position	Date	Shared by
All SUARDIAZ Group personnel	10/12/2018	Email.
All SUARDIAZ Group personnel	19/12/2022	Email and SharePoint. Published on SUARDIAZ Group website.
All SUARDIAZ Group personnel	27/11/2023	Email and SharePoint. Published on SUARDIAZ Group website.

Contents

1. INTRODUCTION..... 3

2. PURPOSE..... 5

3. SCOPE OF APPLICATION 6

4. PROFESSIONAL CONDUCT AND ACTION GUIDELINES 8

 4.1. DISCOVERY AND DISCLOSURE OF SECRETS..... 8

 4.2. EVASION..... 8

 4.2.1. FRAUD 8

 4.2.2. MISAPPROPRIATION 9

 4.3. PUNISHABLE INSOLVENCIES 9

 4.4. DAMAGES..... 9

 4.5. INTELLECTUAL AND INDUSTRIAL COPYRIGHT..... 10

 4.6. MARKET AND CONSUMERS..... 11

 4.7. MONEY LAUNDERING AND RECEIVING..... 12

 4.8. INLAND REVENUE AND SOCIAL SECURITY 12

 4.9. WORKERS' RIGHTS..... 13

 4.10. TERRITORIAL ORGANISATION AND TOWN PLANNING 13

 4.11. NATURAL RESOURCES AND ENVIRONMENT..... 14

 4.12. PUBLIC HEALTH..... 14

 4.13. HAZARDS CAUSED BY EXPLOSIVES OR OTHER AGENTS 14

 4.14. BRIBERY AND INFLUENCE PEDDLING..... 15

 4.15. FALSIFICATION OF CREDIT AND DEBIT CARDS, AND TRAVELLER'S CHEQUES
 15

 4.16. TERRORISM..... 15


5. CRIME PREVENTION AND REDUCTION MEASURES..... 17

6. CRIME CONTROL AND SUPERVISION MEASURES..... 18

7. CONSEQUENCES OF BREACHING THE PROTOCOL 19

8. EVALUATION OF COMPLIANCE AND EFFECTIVENESS OF THE PROTOCOL 20

APPENDIX I. Ratification and Declaration of Commitment..... 21

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

APPENDIX II. Protocol on the Use and Control of the SUARDIAZ Group's IT Resources..... 22

1. INTRODUCTION

With the coming into force of the Penal Code's Organic Law 5/2020, of June 22, which modifies Organic Law 10/1995, of November 23, and in response to numerous international legal instruments demanding a clear penal response on the part of legal entities, Spanish legislation establishes in detail a system of penal responsibility for such.

As a result of the above, legal entities shall be penally responsible for:


- Crimes committed in their name and on their behalf, and for their benefit, by their legal representatives and administrators –de facto and de jure–, and
- Crimes committed, while conducting business activities on their behalf, and for their benefit, by those who, being subject to the individuals mentioned in the previous paragraph, may have done so due to a lack of control over them.

The direct consequence for a company declared penally responsible is the imposition of a penal sanction, which generally consists of a fine. However, it may also include sanctions such as the loss of tax benefits, the suspension of activities, the closure of premises and establishments, or even the dismantling of the legal entity.

In addition to the penalties that may be imposed by the courts, there are other consequences for companies that may prove to be equally onerous for the continuation of its business, such as i) reputational consequences with regard to investors, clients, and suppliers, and ii) economic consequences derived, among others, from the difficulty or impossibility of receiving credit from financial institutions, etc.

Notwithstanding the legal entity's penal responsibility, infringement of this Protocol's provisions may result in disciplinary actions, which could even include dismissal and involve, in accordance with applicable legislation, legal responsibility, both civilly and penally.

In addition to the framework of the recommendations for good corporate governance that is generally recognised in international markets and generally accepted social responsibility principles, GRUPO LOGÍSTICO SUARDIAZ, S.L. and

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

Subsidiary Companies (henceforth, SUARDIAZ Group), an international business group specialising in comprehensive logistics services (Transport of Vehicles and Ro-Ro Cargo, Operation Services Management of Oil Tankers and Supply Barges, Shipping Agent and Husbandry Agent, Freight Forwarder and Multimodal Transport Operator, Customs Agent, Warehousing and Logistics Operator, Rail Transport, Management and Handling of Intermodal Freight at Railway Terminals, Railway Operator, Maritime Auxiliary Services, Manufacture and Assembly of Pipes and Metallic Structures, Welding and Boiler Steel Works in general, among others), is committed to sustainable development and its clients, its human resources and stakeholders, with high standards of quality and respecting the environment, both in Spain and in the different jurisdictions in which SUARDIAZ Group operates.


SUARDIAZ Group highlights its commitment to practices of ethical commerce and compliance, and establishes the fundamental principles that should govern its business: Integrity, Commitment, Responsibility, Excellence, and Sustainability.

It likewise makes known the standards that should govern the conduct of those that form part of the SUARDIAZ Group's team, from management, employees, legal representatives –de facto and de jure– to business partners, interested parties, and stakeholders, when they do business with SUARDIAZ Group.

In relation to its corporate social responsibility, SUARDIAZ Group adheres to the United Nations' Global Compact, confirming its participation as an associated signatory since 2012.

SUARDIAZ Group would like to express its "0" tolerance with regard to any behaviour on the part of those that form part of SUARDIAZ Group that infringes, in some way, the dispositions established in this Protocol.

As a result of all of the above, the SUARDIAZ Group's Board of Directors initially approved on December 10, 2018, this Action Protocol for the Purposes of Crime Control and Prevention and Anti-Fraud (henceforth, the "Protocol") in order to introduce the duties imposed by the reform of the Penal Code and implement its policy for crime prevention and anti-fraud.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edition 03
		27/11/2023


2. PURPOSE

The purpose of this Protocol is to effectively implement the duties of crime and fraud control and prevention imposed on legal entities by the reform of the Penal Code.

This is so in order to guarantee, in relation to third parties and judicial authorities, that both GRUPO LOGÍSTICO SUARDIAZ, S.L. and its Subsidiary Companies, directly or indirectly, exercise the due control that is legally required over their employees, legal representatives, and administrators –de facto and de jure.

With this objective, the Protocol is aimed at:

- a. Sending a categorical message to all its employees, legal representatives, and administrators –de facto and de jure– that it is opposed to, and is determined to tackle, the commission of any crime.
- b. Implementing specific action protocols to prevent and reduce the risk of crimes being committed.
- c. Establishing effective mechanisms for communicating and reporting supposed criminal, fraudulent, or irregular actions, ensuring the confidentiality of the whistleblower, as well as the investigations to clarify the supposed criminal actions.
- d. Establishing permanent control and supervision systems to prevent crimes from being committed.
- e. Introducing action protocols to deal with the commission of crimes.
- f. Adopting mechanisms to evaluate the fulfilment and effectiveness of this Protocol and its updating.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edition 03
		27/11/2023

3. SCOPE OF APPLICATION


This Protocol shall be applicable to all employees, legal representatives, and administrators –de facto and de jure– of both GRUPO LOGÍSTICO SUARDIAZ, S.L. and its Subsidiary Companies, directly or indirectly (henceforth, SUARDIAZ Group); it shall likewise extend to consultants and contractors that work on behalf of and/or in the name of such, interested parties and stakeholders.

SUARDIAZ Group expects all its employees, legal representatives, and administrators –de facto and de jure– to:

- a. Read and understand the regulations stipulated in this Protocol, signing the acknowledgment of receipt attached as Appendix in witness whereof.
- b. Follow such regulations in their daily professional activities.
- c. Seek assistance from the SUARDIAZ Group’s Ethics Unit (as indicated in Section 5 of this Protocol) if they have any queries or need further clarification regarding the application of this Protocol’s regulations.
- d. Report any observed or suspected infringement of the Protocol to the Ethics Unit (as indicated in Section 8 of the Internal Information System Regulation of SUARDIAZ Group).
- e. Extend and promote, as far as possible, its fulfilment among the SUARDIAZ Group’s other employees, and publicise it among its business partners, including the agents, suppliers, distributors, and risk-sharing business partners with whom SUARDIAZ Group has a professional relationship.
- f. Collaborate in clarifying the reported actions, in accordance with this Protocol’s regulations.


SUARDIAZ Group also expects its business partners, including its agents, suppliers, distributors, risk-sharing business partners, stakeholders, and other interested parties to comply with the same or similar principles in their own operations.

Those acting as the SUARDIAZ Group’s legal representatives or administrators –de facto or de jure– have additional responsibilities that go beyond the observance of the Protocol’s regulations. Such ones must promote, as far as possible, and set an

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

example in this regard, the application of the principles contained herein in those companies that represent SUARDIAZ Group.

For its part, SUARDIAZ Group makes available to all its employees, legal representatives, and administrators –de facto and de jure– the necessary tools for settling any queries or clarifications that may arise in the application of this Protocol.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edition 03
		27/11/2023

4. PROFESSIONAL CONDUCT AND ACTION GUIDELINES

4.1. DISCOVERY AND DISCLOSURE OF SECRETS

The SUARDIAZ Group’s employees, legal representatives, and administrators –de facto and de jure– shall abstain from –so as not to discover secrets or violate another person’s privacy without their consent– seizing papers, letters, e-mail messages, or any other personal documents or items, intercepting their telecommunications, or using technical devices for tapping, transmitting, recording, or reproducing sound or images, or any other communication signals.

They shall likewise abstain from, without authorisation, seizing, using, or modifying, to the detriment of third parties, another person’s confidential personal or family data in IT files or media –electronic or telematic– or in any other type of public or private file or register.

Similarly, they shall not access without authorisation, by any means or procedure and by vulnerating the established safety measures, data or IT programmes contained in an IT system, or in part of such, or remain within such against the will of the person that is legitimately entitled to exclude them.


Finally, and in all cases, they shall abstain from disseminating, disclosing, or transferring to third parties any data or facts that, where applicable, they may have discovered, or any images that they may have copied.

In this regard, SUARDIAZ Group has already implemented specific measures in relation to the processing of data collected by SUARDIAZ Group in the normal operation of its activities, in order to comply with the Data Protection legislation in force.

4.2. EVASION

4.2.1. FRAUD

The SUARDIAZ Group’s employees, legal representatives, and administrators –de facto and de jure– shall abstain from seeking their personal gain by employing deceit to mislead another person, inducing him/her to act to their own, or to another’s, detriment.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

Neither shall they, i) by falsely claiming to have the authority to do so, alienate, place a lien upon, or lease personal or real property to another person to his/her detriment, or that of a third party, ii) dispose of personal or real property while hiding the existence of any tax burden on it, or after alienating it as free, place a lien upon it or alienate it once again after the final transfer to the purchaser, to the detriment of the latter or a third party, and iii) award a simulated contract to the detriment of another person.

Neither shall they, in relation to any kind of legal proceedings, manipulate the evidence that the SUARDIAZ Group plans to base its allegations on, thereby misleading the Judge or Court so that they decree a ruling that is favourable to the SUARDIAZ Group's interests.

4.2.2. MISAPPROPRIATION

The SUARDIAZ Group's employees, legal representatives, and administrators –de facto or de jure– shall not appropriate or embezzle money, items, securities, or any personal property or assets that may have been received as a deposit, commission, or to administer, or any other bond that must be handed over or returned, or deny that they have received such.


They shall likewise abstain from committing any type of fraud by using electricity, water, gas, telecommunications, or other elements, energy, or fluids that do belong to them, by employing the mechanisms installed for this purpose, maliciously altering the indications or meters, or employing any other clandestine elements.

4.3. PUNISHABLE INSOLVENCIES

The SUARDIAZ Group's employees, legal representatives, and administrators –de facto and de jure– shall not try to avoid satisfying any of the SUARDIAZ Group's obligations or debts, nor by seizing the SUARDIAZ Group's assets to the detriment of its creditors, or making use of its assets or generating obligations so as to delay, hinder, or impede the effectiveness of an embargo, executive or compulsory procedure, judicial, extrajudicial, or administrative that has been initiated or is expected to be.

4.4. DAMAGES

The SUARDIAZ Group's employees, legal representatives, and administrators –de facto and de jure– shall abstain from erasing, damaging, deteriorating, altering, suppressing, or making inaccessible data, IT programmes, or electronic documents

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

that do not belong to them, nor shall they hinder or interrupt, without authorisation, the functioning of a IT system that does not belong to them, by entering, conveying, damaging, erasing, deteriorating, altering, suppressing, or making inaccessible IT data.

4.5. INTELLECTUAL AND INDUSTRIAL COPYRIGHT

The SUARDIAZ Group’s employees, legal representatives, and administrators –de facto and de jure– shall abstain from, so as not to obtain personal gain to the detriment of a third party, reproducing, plagiarising, distributing, or publicly communication, in full or in part, a scientific work, or its transformation, stored in any type of media or communicated by any means, without the authorisation of the corresponding intellectual copyright owners or their transferees.


Neither shall they intentionally export or store copies of such works, productions, or attachments without the corresponding authorisation.

Likewise, they shall not manufacture, import, distribute, or dispose of any means specifically aimed at facilitating unauthorised suppression or neutralising any technical device that has been used to protect IT programs or any of the other works, interpretations, or attachments described in the first section.

The SUARDIAZ Group’s employees, legal representatives, and administrators –de facto and de jure– shall abstain from, for industrial or commercial purposes, and without the consent of the owner of a patent, utility model, patented procedure, objects protected, in favour of a third party, by a model or industrial blueprint or plan of a semiconductor product, and being aware of its registration, manufacturing, importing, possessing, using, offering, or commercialising objects protected by such rights.

They shall likewise abstain, for agricultural or commercial purposes, without the consent of the owner of a plant variety right and being aware of its registration, producing or reproducing, making preparations with a view to production or reproduction, selling or otherwise commercialising, exporting or importing, or possessing for any of the aforementioned purposes, plant material for reproducing or multiplying a protected plant variety in accordance with the legislation governing plant variety protection.

They shall likewise abstain from, for industrial or commercial purposes, without the consent of the owner of industrial copyright registered in accordance with brand legislation and being aware of its registration, reproducing, imitating, modifying, or otherwise usurping a distinctive sign (brand, commercial name or domain) that is

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

identical to, or can be mistaken for, that of the former, to distinguish the same or similar products, services, activities, or establishments for which the industrial copyright has been registration.

4.6. MARKET AND CONSUMERS

The SUARDIAZ Group’s employees, legal representatives, and administrators –de facto and de jure– shall abstain from investigating the secrets of third-party companies and, consequently, from seizing, by any means, data, written or electronic documents, IT media, or other related objects, and, where applicable, from disseminating, disclosing, or transferring the discovered secrets to third parties.

Likewise, they shall not disseminate, disclose, or transfer a company secret that they are legally or contractually bound to keep confidential.

The SUARDIAZ Group’s employees, legal representatives, and administrators –de facto and de jure– shall abstain from removing from the market raw materials or essential products with the intention of cutting the supply of such to a certain sector, alter prices, or cause serious harm to consumers.


Likewise, in relation to their offers or advertising of products or services, they shall not make false claims or express uncertain characteristics regarding such, so as not to cause serious harm to consumers.

Likewise, they shall not alter or manipulate the automatic apparatuses that measure the cost or price of products or services, with a view to overcharging.

The SUARDIAZ Group’s employees, legal representatives, and administrators –de facto and de jure– shall abstain from using violence, threats, or deceit to try to alter prices that should be set by free competition among products, goods, securities, or financial instruments, services, or any other personal or real property under consideration for contracting.

Neither shall they spread news or rumours, by themselves or by way of a means of communication, regarding persons or companies in which they knowingly provided completely or partially false economic data, with the objective of altering or maintaining the trading price of a security or financial instrument.

Likewise, they shall not use privileged information to carry out transactions or order operations that are liable to provide deceitful indications regarding supply, demand, or the price of securities or financial instruments, or to ensure, by using such

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

information, by themselves or in agreement with others, a dominant market position in relation to such securities or instruments, with the objective of fixing their prices abnormally or artificially.

Neither shall they use valuable information about the trading price of any kind of securities or instruments negotiated in an official or recognised organised market, which they have obtained during their work, or share such for economic gain for themselves or a third party.

4.7. MONEY LAUNDERING AND RECEIVING

The SUARDIAZ Group’s employees, legal representatives, and administrators –de facto and de jure– shall abstain from helping those responsible for committing a crime regarding assets or the socioeconomic order, from benefiting from the effects of such, or from receiving, acquiring, or hiding such effects for any purpose.

Neither shall they acquire, possess, use, convert, or transfer assets resulting from criminal activities, or carry out any actions to hide or cover up their illicit origin, or help anyone that has participated in the infringement to evade the legal consequences of their actions.


Likewise, they shall not hide or cover up the real nature, origin, location, destination, movement, or right to assets or the ownership of such.

4.8. INLAND REVENUE AND SOCIAL SECURITY

SUARDIAZ Group respects in all cases the tax and labour regulations that apply to it and shall abide by the regulations contained therein.

The SUARDIAZ Group’s employees, legal representatives, and administrators –de facto and de jure– shall not, while carrying out their professional activities, defraud in any way, in the name and on behalf of SUARDIAZ Group, the state, regional or local Inland Revenue, nor the European Treasury, by evading the payment of taxes, withholdings, or amounts that should have been withheld, or payments on account of remunerations in kind, unduly obtaining refunds or enjoying tax benefits in the same way.

Likewise, they shall not defraud, in the name or on behalf of SUARDIAZ Group, the Social Security system, evading the payment of its contributions and joint quotas, unduly obtaining refunds of such, and unduly enjoying any kind of deduction.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

4.9. WORKERS' RIGHTS

The SUARDIAZ Group's executives, legal representatives, and administrators –de facto and de jure– shall abstain from imposing on its workers, by means of deceit or by abusing a situation of need, labour or Social Security conditions that harm, suppress, or restrict their legally, conventionally, or contractually recognised rights. Neither shall they maintain such conditions whenever ownership of a company is transferred.

Neither shall they recruit individuals or oblige them to leave their jobs by offering them deceitful or false employment or working conditions, or employ foreigners without a work permit.


They shall abstain from discriminating, in any way, anyone due to their ideology, religion or beliefs, due to their belonging to an ethnic group, race, or nation, gender, sexual orientation, family situation, illness or disability, due to their status as legal or trade union representatives of workers, due to their family relationship with other workers of the Group, or for their use of any of Spain's co-official languages. Neither shall they impede or limit, by means of deceit or the abuse of a situation of need, the freedom of association or the right to strike.

The SUARDIAZ Group's employees, legal representatives, and administrators –de facto and de jure– shall comply with occupational risk prevention regulations and shall provide the necessary means so that workers can carry out their activities with appropriate health and safety measures, all this in strict compliance with the regulations stipulated in the SUARDIAZ Group's Occupational Risk Prevention Plan, revised on October 1, 2018, and any updates that are made, in order to attain, among others, the goal established therein of Zero Accidents.

In this regard, SUARDIAZ Group has implemented specific occupational risk prevention plans in its subsidiaries, encompassing the fields of Safety, Health, Ergonomics and Applied Psychology, and Health Surveillance, all of this in compliance with the applicable legislation in force.

4.10. TERRITORIAL ORGANISATION AND TOWN PLANNING

The SUARDIAZ Group's employees, legal representatives, and administrators –de facto and de jure– shall abstain from conducting unauthorised building work on land set aside for roads, green spaces, public property, or legally or administratively protected places due to their scenic, ecological, artistic, historical, or cultural value, or sites that enjoy special protection for the same reasons.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

In all its activities, SUARDIAZ Group shall obtain beforehand all licences, permits, and authorisations required in each case.

4.11. NATURAL RESOURCES AND ENVIRONMENT

SUARDIAZ Group hereby declares that sustainable development, i.e., satisfying the growing needs of the present without compromising future generations' possibilities, is one of the pillars on which its growth is based. In this regard, it has the knowledge and dedication required to promote the highest environment standards in industry, with the reduction of energy consumption and emissions being its top priority.


Based on the above, the SUARDIAZ Group's employees, legal representatives, and administrators –de facto and de jure– shall abstain from contravening general environmental protection laws or regulations, by producing, directly or indirectly, emissions, waste, radiation, extractions or excavations, siltation, noise, vibrations, injections or deposits, in the atmosphere, soil, subsoil, or inland, underground or maritime waters, including the deep sea, even in transborder areas, as well as water catchments that may seriously harm the balance of natural systems and/or human health.

4.12. PUBLIC HEALTH

The SUARDIAZ Group's employees, legal representatives, and administrators –de facto and de jure– shall not cultivate, make, traffic in, promote, favour, or facilitate the illegal consumption of toxic drugs, narcotics, or psychotropic substances, or possess them for such purposes.

4.13. HAZARDS CAUSED BY EXPLOSIVES OR OTHER AGENTS

The SUARDIAZ Group's employees, legal representatives, and administrators –de facto and de jure– shall not, except in compliance with applicable sectorial national and European legislation and in strict adherence to the SUARDIAZ Group's internal regulations that apply in each case as well as any updates that are made to such, manufacture, handle, transport, possess, or sell explosives, corrosive, inflammable, toxic, or asphyxiating substances, or any other materials, apparatuses or devices that may wreak havoc, infringe established safety regulations, specifically endangering human life or health, or the environment; neither shall they facilitate their effective loss or removal.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

By virtue of the above, the SUARDIAZ Group's employees, legal representatives, and administrators –de facto and de jure– shall abstain from illegally producing, importing, exporting, selling, or using ozone-depleting substances.

4.14. BRIBERY AND INFLUENCE PEDDLING

The SUARDIAZ Group's activity obliges it to have periodical contact with governments, and international and regional organisms. It therefore radically and firmly requires all its employees, legal representatives, and administrators –de facto and de jure– to deal with administrations with the utmost transparency and honourability.

SUARDIAZ Group is radically against influencing individuals outside the company to obtain any type of benefit by means of illicit and/or non-ethical practices, as well as satisfying their requests.

The SUARDIAZ Group's employees, legal representatives, and administrators –de facto and de jure– shall not participate, at any time, in giving or offering, either directly or indirectly, gifts, presents, offers, or promises, or influencing, making use of any situation derived from their personal relationship, authorities, including foreigners or international organisations, or any person at the service of any public or private entity, as well as private individuals, with the intention of illicitly obtaining or maintaining any undue business or other advantages.


Likewise, the SUARDIAZ Group's employees, legal representatives, and administrators –de facto and de jure– are not permitted to accept gifts, presents, offers, or promises from the persons described in the previous paragraph, when this affects, or can affect, their integrity or independence.

4.15. FALSIFICATION OF CREDIT AND DEBIT CARDS, AND TRAVELLER'S CHEQUES


The SUARDIAZ Group's employees, legal representatives, and administrators –de facto and de jure– shall abstain from altering, copying, reproducing, or in any way falsifying credit or debit cards, or traveller's cheques.

4.16. TERRORISM

The SUARDIAZ Group's employees, legal representatives, and administrators –de facto and de jure– shall abstain, either directly or indirectly, from supplying or collecting funds with the purpose of being used, or knowing that they will be used,

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

in full or in part, to commit any crimes related to the possession, traffic, and storage of arms, munition, or explosives, and crimes of terrorism, or to passing them on to a terrorist organisation or group.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edition 03
		27/11/2023

5. CRIME PREVENTION AND REDUCTION MEASURES

SUARDIAZ Group promises to provide the contents of this Protocol and, where applicable, the corresponding updates, on an individual, personalised basis, to each and every one of its workers, legal representatives, and administrators –de facto and de jure.


It likewise makes available to the aforementioned persons a communication channel to use to obtain advice or clarification regarding the contents of this Protocol, or its application while carrying out their daily work.

The reporting of any supposed criminal, fraudulent, or irregular actions described in this section may be carried out by any of the channels established in the Internal Information System Regulation of SUARDIAZ Group.

The SUARDIAZ Group's Ethics Unit shall conduct any preliminary investigations that it considers necessary to clarify the facts and, where applicable, will transfer the complaint to the Internal Information System Manager in order to initiate the investigation procedure detailed in the Internal Information System Regulation of SUARDIAZ Group.


The Unit guarantees that it shall investigate every complaint regardless of its characteristics and, where applicable, the amount involved, as soon as possible, guaranteeing at all times the confidentiality of the whistleblower and the defendant, as well as all the investigations carried out to clarify the facts. Likewise, SUARDIAZ group shall not take any reprisals, directly or indirectly, against those who have reported an irregular situation in strict compliance with the terms of Law 2/2023, of February 20, as well as the SUARDIAZ Group's Internal Information System Regulations.

The Internal Information System Manager – if permitted by the applicable legislation and in accordance with what is stipulated in Appendix II– shall employ the mechanisms that it deems necessary to investigate the reported facts. In relation to the aforementioned, the SUARDIAZ Group's employees, legal, representatives, and administrators –de facto and de jure– shall collaborate with the Internal Information System Manager as required in the investigation of the facts that, where applicable, have been reported.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edition 03
		27/11/2023

6. CRIME CONTROL AND SUPERVISION MEASURES

The Unit, at its own initiative or in view of the communication of the complaint(s) made, shall be carried out in accordance with the following regulations established in the Internal Information System Regulations of SUARDIAZ Group.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edition 03
		27/11/2023

7. CONSEQUENCES OF BREACHING THE PROTOCOL

In view of the results of the procedure described in the previous section, the Unit shall send the said report to the Board of Directors and to the Corporate Human Resources Director of SUARDIAZ Group, so that they can adopt the appropriate agreements and, where applicable, inform the corresponding police and/or judicial authorities.


Otherwise, the investigation report shall be considered closed.

The imposition of the sanctions included in this Protocol shall be conducted under parameters of justice, non-discrimination, and proportionality, in accordance with what is stipulated in the applicable legislation at each moment.

The Ethics Unit and the Internal Information System Manager shall always guarantee the maximum respect for the rights of those supposedly involved in a possible infringement of this Protocol.

The Ethics Unit and the Internal Information System Manager shall therefore guarantee a thorough analysis of the supposed infringements that have been reported to ensure their truthfulness.

Nonetheless, it is hereby notified that resorting to this procedure knowing that the reported facts are false, or showing utter contempt for the truth, may result in penal or civil responsibilities as stipulated in current legislation.


	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edition 03
		27/11/2023

8. EVALUATION OF COMPLIANCE AND EFFECTIVENESS OF THE PROTOCOL

The Board of Directors and the Ethics Unit shall jointly and periodically evaluate the degree of compliance with the Protocol, and, in any case, the Board of Directors shall provide an annual update on the results of such.

In the light of the results of the above, the Protocol shall be revised and, where applicable, modified and updated as necessary, also taking into account possible modifications in applicable legislation and any suggestions and proposals that, where applicable, are made by the SUARDIAZ Group’s workers, legal representatives, and administrators –de facto and de jure– by way of the communication channel contemplated in Section 5 of this Protocol.

Any revision or update that changes this Protocol, even when required by the national legislation of any of the countries in which SUARDIAZ Group operates, must be approved by the Board of Directors of SUARDIAZ Group and shall be made available to all employees, legal representatives, and administrators –de facto and de jure.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edition 03
		27/11/2023

APPENDIX I. Ratification and Declaration of Commitment

I hereby ratify that I have read and understood the contents of the *“Action Protocol for the Purposes of Crime Control and Prevention and Anti-Fraud.”*

I likewise promise to implement the conduct guidelines and procedures established therein in my everyday work.


Mr/Ms:

Name and Surname:

Date:

Signature:

After receiving the contents of this *Protocol*, you should deliver this acknowledgement of receipt to the SUARDIAZ Group’s Corporate Human Resources Department.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edition 03
		27/11/2023

APPENDIX II. Protocol on the Use and Control of the SUARDIAZ

Group's IT Resources

I.- INTRODUCTION

SUARDIAZ Group, in light of the importance, extensiveness, and complexity that the use of IT resources has acquired in the work environment, deems it necessary to establish regulations and procedures to govern their use and control within the Group.

The IT resources that SUARDIAZ Group makes available for its workers must be used for carrying out their work.

Regardless of this being the main use and purpose of the IT resources, SUARDIAZ Group acknowledges that its workers may use such for personal use under a restrictive and exceptional criterion.


Moreover, SUARDIAZ Group hereby declares that since these are labour resources, it may exercise over them any necessary measures to manage, administer, and control them, while always respecting the workers' right to privacy, based on the administrative power recognised in Article 20 of Royal Legislative Decree 1/1995, of March 24, which approves the consolidated text of the Law of the Workers' Statute.

The rules established in this Protocol must be followed by the entire workforce from now on.

II.-GENERAL CONDITIONS FOR USING THE IT SYSTEM AND WORKSTATIONS


- The SUARDIAZ Group's IT system resources must not be used for private purposes, or any other purpose other than what is strictly labour-related, regardless of their possible use for private purposes within the terms stipulated in this Protocol.
- No IT products can be installed in workstations. This affects both products included in CD-type media, USB memories or similar, and those received by e-mail or downloaded from the Internet.

All applications required for the correct fulfilment of labour activities shall only be installed by authorised personnel of the Corporate IT Department.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

- The «EMPRESAS_C010_RazonSocial» IT system is protected against IT viruses by an antivirus. If any issues arise in this regard, the user is obliged to immediately notify the persons in charge of the SUARDIAZ Group's Corporate IT Department and collaborate as required to solve the incident, following the established regulations for managing incidents.
- It is strictly forbidden to fraudulently access, or try to access, other public network systems, as well as unauthorised resources within the «EMPRESAS_C010_RazonSocial» IT network itself.
- It is forbidden to record corporate data in the hard disks of local workstations, except in specific cases authorised by SUARDIAZ Group. All information used in carrying out the everyday work of SUARDIAZ Group shall be stored on the corresponding network disk.
- The personal computer must not be left unattended while they are connected to the IT system. If the user has to leave his/her workstation, he/she must disconnect the PC from the system, or duly block it.
- Any physical device (such as printers, modems, photocopy machines, scanners, and other peripherals), whether connected or not to the PC, must be placed so as to prevent unauthorised persons from accessing the information. The persons in charge of each workstation shall use such devices with due diligence and ensure the confidentiality and integrity of the information during their use.

If any of these resources are shared by «EMPRESAS_C010_RazonSocial» personnel, each Worker shall exercise due diligence so that no information, regardless of its kind, shall be stored in such physical devices (i.e., papers in a shared printer).
- When a person leaves his/her workstation, for whatever reason, no documents –confidential or otherwise– should be left there.
- It is forbidden to reveal to any person outside of the organisation, information that a person has accessed while carrying out his/her work, without due authorisation. Such information must only be used as required to carry out their work; it is forbidden to use it in any other way, or for other purposes.
- Nobody outside of the organisation shall be given any storage elements containing information that has been accessed during a person's work, without due authorisation.
- Access, or any other kind of IT processing, is not permitted in the case of data that is not required to perform a person's work correctly within the organisation.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

- The obligation to comply with the above commitments even applies after a person has terminated his/her working relationship with SUARDIAZ Group.
- The backup copy of any data stored in a portable IT device is the user's responsibility.
- The worker shall be responsible, with regard to «EMPRESAS_C010_RazonSocial» and third parties, for any damage that may be caused to either of them due to non-compliance with the aforementioned commitments, and must compensate SUARDIAZ Group for any compensation, sanctions, or demands that they are obliged to satisfy as a result of such non-compliance.


III.- PORTABLE DEVICES

When travelling outside of the usual workplace, the following precautions must be observed with regard to portable devices (laptop, tablet, smartphone, mobile phone, etc.):

- Avoid leaving them in visible places and/or places that can be easily accessed by unauthorised personnel.
- Avoid keeping them in compartments or storage places without a lock.
- Avoid checking them in when using means of transport.
- Avoid leaving them switched on, without the corresponding protection mechanisms.
- The worker shall set up, in the IT equipped provided by SUARDIAZ Group, an access security code to protect the stored information in case of loss or theft. In the case of laptops, this code shall be set up by SUARDIAZ Group and notified to the worker in timely fashion. Each worker is responsible for keeping the assigned access codes secret and confidential; it is forbidden to reveal them to other employees or third parties.

If it is necessary to access any of the devices that the SUARDIAZ Group's Corporate IT Department has assigned to a worker that is absent, the Group may access such by notifying this circumstance to the worker.

- Prevent any technical manipulation of such by unauthorised personnel.
- Any confidential information belonging to SUARDIAZ Group must not be accessed on board a plane or in public places, unless the person is absolutely sure that he/she is the only one that can read the information that appears on the device's screen.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

- It is forbidden to use start-session command or automatic initialisation sequences that enable unauthorised third parties to access an account without knowing the password.
- Portable IT devices must not be left alone when remotely connected to the SUARDIAZ Group's corporate network, even if they are physically safe.
- Updated antivirus software (including virus definitions) must always be installed with the automatic monitoring option activated. Any media or files from outside the organisation must be examined before opening them.
- The loss of a portable IT device must be notified to the person in charge of security, in accordance with the policies for managing incidents, as soon as possible, but no later than twenty-four hours after the loss.

IV.- CONTROL FOR ACCESSING THE IT SYSTEM'S RESOURCES AND DATA


Access control refers to the mechanism that, based on identification, enables a user to access data and/or resources of the SUARDIAZ Group's IT systems.

This access is only and solely permitted in accordance with the needs derived from the user's professional functions and obligations. To that end, there exist appropriate technical mechanisms, which guarantee a level of access adapted to each user's profile.

As a general rule, a user's access shall be restricted to all resources in the SUARDIAZ Group's IT system, except for the authorisations specifically assigned to him/her due to the work that they carry out within the organisation. Such authorisations shall be assigned to him/her by the person in charge of the area to which the user belongs or, in his/her absence, by the Corporate Department of Human Rights, which will send the request in writing to the Corporate IT Department, following the established procedure. The personnel of the SUARDIAZ Group's Corporate IT Department shall be the only ones empowered to manage the access to the system's data and resources.

This procedure is valid for both registering new users, and for changes in access due to a change in a user's professional functions.


Persons that have access to sensitive information, or who receive information from clients, suppliers, etc., in any kind of media, shall be obliged to fulfil the security and confidentiality regulations and procedures in force at any given time.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023


Unauthorised access to files by users is a breach of the security measures and may result in SUARDIAZ Group being penalised by the Data Protection Agency.

V.- CONDITIONS OF E-MAIL USE

- Users are responsible for all activities carried out with the e-mail accounts provided by SUARDIAZ Group.
- Professional e-mails must be sent from the professional e-mail addresses assigned to workers, and not from private e-mail addresses.
- It is forbidden to facilitate and/or allow the use of a professional e-mail account by unauthorised personnel.
- Users must be aware of the risks involved in the incorrect use of e-mail addresses provided by SUARDIAZ Group. E-mail messages convey information in their headers –which are hidden in principle– that provide additional information about the sender. They should therefore take into account any possible repercussions (such as harm to the institutional image) that could arise from an incorrect use of this resource.
- The e-mail services provided by SUARDIAZ Group must be used for strictly work-related purposes. Exceptionally, they may be used for personal matters as long as this does not interfere with the performance of the service itself, the user's labour activities, the service administrators, or does not involve a high cost for the Group. In any case, such usages are subject to the rules on personal use that is stipulated in Section VII below.
- It is forbidden to use e-mail boxes from other Internet service providers in IT equipment provided by SUARDIAZ Group. The following is especially forbidden: the use as mail routers of equipment other than that provided by the Group, sending messages with addresses that have not been assigned by the institution's responsible persons, and the manipulation of the headers of outgoing e-mails.
- The SUARDIAZ Group's IT system is protected against IT viruses by an antivirus. Responsibility for communicating to those in charge of the system any incident that arises in this regard lies with each user, as well as opening a suspicious e-mail or a virus message sent by the antivirus.
- It is advisable not to open any e-mail messages suspected of containing malware (e.g., IT viruses). If in doubt, it is necessary to consult the specialised personnel of the SUARDIAZ Group's Corporate IT Department.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

- E-mail must not be used to send user access codes or passwords, as well as data related to electronic payment systems (credit cards, etc.) that belong to SUARDIAZ Group.
- E-mail is a tool for exchanging information between people and must not be used as a tool for sharing information. There are more appropriate and effective channels available for this, in which case those in charge of the service should be contacted.
- E-mail must not be sent to persons that do not want to receive it. If such messages satisfy certain requirements, they may be considered spam, which is forbidden by our country's current legislation. If «EMPRESAS_C010_RazonSocial» receives any complaints about such practices, the corresponding penalties shall be imposed.
- It is completely forbidden to use e-mail for any of the following activities:
 - Carrying out commercial and/or financial activities not expressly authorised by SUARDIAZ Group.
 - Sending slanderous, defamatory, intimidating messages, or any the kind that may be interpreted as such.
 - Participating in passing on chain letters, pyramid schemes, or similar.
 - Distributing messages with content that SUARDIAZ Group deems inappropriate.
 - Falsifying e-mail headers.
 - Collecting e-mail from the boxes of other Internet service providers without express authorisation.
 - Obtaining or spreading material with legal or immoral content (defence of terrorism, piracy, pornography, xenophobia, threats, rackets, virus, malware, hacking, etc.).
 - Sending one's own e-mail by means of third-party accounts without the owner's consent.
 - Carrying out attacks in order to disable or hinder IT systems (denial-of-service attacks) aimed at a user of an e-mail system itself, as well as sending a large of messages per second (mail bombing) or any other variation designed to paralyse the service by saturating its lines, the server's CPU capacity, available disk space in servers or terminals, or any other similar practice.

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

- Sending messages that compromise the SUARDIAZ Group's reputation to discussion forums, distribution lists, and/or newsgroups.


VI.- CONDITIONS OF INTERNET USE

- The SUARDIAZ Group's Internet network is work-related and must not be used for other purposes, without prejudice of its possible use for private purposes that must be carried out in accordance with the terms established herein. Users are the only ones responsible for any Internet sessions initiated from their workstations.
- In no case can the IT's browser configurations (Internet options) be modified, nor can servers or ports be activated without authorisation from those in charge of security.
- The use of images (such as GIF, JPG, BMP, or TIFF formats, among others), audio (mainly WAV and MP3 formats) and video (MPG, DivX, AVI, RAW, or similar) for purposes other than the SUARDIAZ Group's work activities must be avoided, since the size of these files saturates communication channels and decreases the transmission speed, thereby harming the performance of the network as a whole.
- It is expressly forbidden to access, download, and/or store in any kind of media, illegal or inappropriate websites or contents (xenophobic, pornographic, sexually explicit, etc); the image, sound, or video formats listed as examples in the previous paragraph; viruses and malware, and, in general all kinds of programmes and/or plug-ins without being expressly authorised by the security coordinator.
- It is forbidden to use IRC services (chat channels) for purposes unrelated to the SUARDIAZ Group's activities, either by accessing websites that provide such, or using applications installed in ITs (such as MS Messenger, TOM, Yahoo!, ICQ, or similar). Neither is it permitted to access online gambling websites or download any similar device.

VII.- PRIVATE E-MAIL USE

The SUARDIAZ Group's workers can use e-mail for private purposes within reasonable, moderate limits.

SUARDIAZ Group shall consider e-mail to be private, for all purpose and expressly with a view to controlling the use of IT resources, when the user writes "PERSONAL Ethics Unit

	ACTION PROTOCOL FOR THE PURPOSES OF CRIME CONTROL AND PREVENTION AND ANTI-FRAUD OF SUARDIAZ GROUP	PT1.1_1
		Edición 03
		27.11.2023

AND CONFIDENTIAL” (in capital letters) in the subject line. The lack of a reference to “PERSONAL AND CONFIDENTIAL” shall mean that the sent e-mail shall be processed as if it were strictly work-related. It can therefore be inspected by SUARDIAZ Group in the terms stipulated herein for such communications.

Employees, Personnel Delegates, and members of the Works Committee are likewise expressly authorised to use e-mail in order to inform and consult the Workers’ Legal Representatives, as recognised in the Consolidated Text of the Workers’ Statute.

VIII.- CORPORATE CONTROL OVER THE USE OF IT RESOURCES

SUARDIAZ Group may employ the mechanisms that it deems necessary to ascertain the scope, frequency, recipient, content, and, general, the use being made of IT resources, including Internet access.

In relation to e-mail, SUARDIAZ Group may inspect the contents of those that are not marked as “PERSONAL AND CONFIDENTIAL,” as indicated in Section VII above, in the following cases:

- When there are reasonable indications that a crime or offence is being committed using e-mail.
- When there are reasonable indications of abuse or inappropriate use of an e-mail message, address, or any other reference, on the part of the user as the sender or recipient.
- When it is reasonable to presume the existence of direct or indirect harm for SUARDIAZ Group caused by e-mail, or for other employees, clients, suppliers, advisers, or persons closely linked to the Group in any other capacity.

If possible, e-mail inspections shall be notified to the worker involved before they are carried out, informing him/her of his right to be present for such.

Please sign in duplicate all pages as acknowledgement of receipt.

In «CENTROS_C010_POBLACION» at «PERSONAL_C010_ FechaAntiguedad»

**RECEIVED,
Mr/Ms**