POLICY ON THE USE OF TECHNOLOGY RESOURCES

INDEX

1 INTRODUCTION

Grupo IGNIS (or the "**Company**") undertakes to carry out all aspects of its activity fulfilling the highest legal and ethical standards. To this end the Company has implemented this Policy on the Use of Technology Resources (hereinafter the "**Policy**") as a way to prevent bribery, avoiding irregular conduct and enabling Grupo IGNIS to respond promptly and effectively to any information required to be provided about its behaviour

This Policy is developed on the basis of the Company's mission, vision and values and is aligned with the rest of Grupo IGNIS's internal policies and codes.

All employees, managers, directors of Grupo IGNIS or anyone acting in its name and in general, any member of Grupo IGNIS (hereinafter, the "**Employees**" or in singular the "**Employee**") will adhere to the Policy and all other policies and internal codes previously approved by the Company for the sake of avoiding and detecting the commission of any unlawful act.

Grupo IGNIS shall make the Policy available to all Employees, which shall be subject to the necessary actions for its communication, implementation, training and awareness-raising.

2 SCOPE OF APPLICATION

The Policy is addressed to directors, managers and, in general, to all Grupo IGNIS's personnel (hereinafter, "Employees") in the exercise of their activity, regardless of the type of contract that determines their employment and/or professional relationship, or the place where they carry out their work.

The Policy is mandatory for all Employees and its observance does not exempt from compliance with any other applicable rules under the laws in force in the areas where Grupo IGNIS operates.

The provisions contained in this Policy and in the Group's other policies are subject to the regulations in force in each country. In the event of any discrepancy between this Policy and the Group's other policies and the regulations in force in each area, Grupo IGNIS's *Compliance Officer* must be consulted in advance.

3 GENERAL RULES FOR THE USE OF TECHNOLOGY RESOURCES.

For the purposes of this Policy, the term "Technology Resources" refers to those technological resources acquired by the Grupo IGNIS and which may be made available to the Employee as a work tool, such as:

- Computers, application servers, remote access terminals, desktop or laptop computers, tablets, fax machines, USB devices, external hard disks and similar or equivalent devices.
- Any software application or programme, networks and systems.
- Internet services, Intranet, Group social networks, e-mail and instant messaging.
- Accounts that give access to the use of hardware, software and information systems, including cloud systems and services contracted by Grupo IGNIS.
- Fixed or mobile devices, smartphones, GPS, etc.
- Drones, robots, *chatbots,* intelligent vehicles and sensors.
- Any other technological element or innovation that may hereafter be acquired by Grupo IGNIS, such as artificial intelligence or *blockchain* software, and made available to the Employee for the performance of his or her duties.

Below is a list of the general rules that must be complied with by Employees in the use of Technology Resources:

Professional use	✓ Technology Resources must be intended for the performance of the services for which the Employee was hired, and must be used in a manner appropriate to their nature and professional purposes.
Right of inspection	✓ Technology Resources and the information contained therein, as working instruments, are subject to inspection, monitoring and auditing, within the limits of the regulations in force. ✓ In the event of sick leave or illness, the Employee shall provide the information contained in the Technology Resources he/she uses to the Employee who replaces him/her. If the former has not provided them, Grupo IGNIS is authorised to do so in accordance with the previous point. ✓ Grupo IGNIS may withdraw the Technology Resources assigned to the Employee in order to ensure the Company's interest, and the Employee must immediately make them

	available to the Group when requested to do so.
Access permissions	✓ Access permissions to Technology Resources and to Grupo IGNIS own information shall be granted so that each Employee has access only to the resources and information necessary for the performance of his or her duties. ✓ Employees must not access the Technology Resources assigned to other Employees or the professional information contained therein, unless expressly authorised by Grupo IGNIS.
Remote connections	✓ Remote connections by Employees to Grupo IGNIS network or information shall be made through the Technology Resources intended for this purpose, these being the only permitted means of access, and always with prior authorisation from the Systems Department. ✓ All technological equipment belonging to persons outside Grupo IGNIS who intend to connect remotely to Grupo IGNIS network or to Grupo IGNIS information requires prior authorisation from the Systems Department, and must have implemented and updated controls for the detection, prevention and correction of malicious code.
Care and protection	✓ Each user shall take care of the Technology Resources assigned to him/her: • Preventing shocks and exposure to extreme temperatures. • Exercising responsible surveillance of them outside Grupo IGNIS premises. • Preventing access and use by third parties. • Avoiding the downloading and/or use of software or executable files of unknown or non-corporate origin, without the express authorisation of the IT department. • Engaging in such other conduct as is necessary for the purpose of this Policy.

4 SPECIFIC RULES FOR USE

4.1 Equipment

Equipment (or hardware): the set of materials that make up an information system: desktop or laptop computers, fax machines, printers, monitors, USB devices, external hard disks, memory cards, tablets, fixed telephones, mobile phones or similar or equivalent devices.

The rules for the use of Equipment are detailed below:

Installation and maintenance	✓ The Systems Department shall be responsible for the installation of new Equipment, as well as for its maintenance. To this end, Employees may not make any changes, manipulations or modifications to the Equipment without the express authorisation of the Systems Department.
Loss or theft	✓ In the event of loss or theft of a Device (e.g. laptop) owned by Grupo IGNIS, the Employee must immediately inform the Systems Department, which will immediately inform the Data Protection Officer (DPO) so that the appropriate measures can be taken in accordance with the regulations in force.
Use of External Resources	✓ The Employee shall preferably work with the Technology Resources provided by Grupo IGNIS. ✓ Should it be necessary for the Employee to introduce or use technological means other than those provided by Grupo IGNIS for the performance of his or her duties, prior authorisation from the Systems Department shall be required. These technological means shall comply with the technical and security requirements established by the Systems Department and shall respect the rules set out in this Policy. ✓ The connection of the Employee's own technological means to the corporate network is prohibited without the express authorisation of the Systems Department.

4.2 Rules for the use of software

Software: set of logical elements of an information system, such as applications, programs, operating system, databases, etc.

The rules for the use of softwares are detailed below:

Procurement	✓ The software necessary for Grupo IGNIS's activity will be contracted in accordance with the procedures in force.
Installation and use	✓ Each Employee shall be provided with the software deemed necessary for the performance of his or her duties. ✓ Employees shall justify requests for Software installation, which shall be approved in accordance with the procedures in force. ✓ It is prohibited: • To install, without prior authorisation from the Systems Department, any software or computer application. • To access and use unlicensed or "pirate" software, as this is considered to be unlawful conduct that can lead to serious criminal liability, as well as clearly endangering both computer equipment and the information contained therein. • To install digital certificates that can be used to represent Grupo IGNIS, without the necessary authorisations. • To copy, without authorisation, the Software or applications installed on the Technology Resources or to try to decompile them, to access their source code or to access them by unauthorised means. • To use any Software to disable or bypass the security measures and controls established by Grupo IGNIS or to perform actions intended to circumvent such controls.
Maintenance	✓ Software maintenance shall cover its entire life cycle. The Employee may not carry out any maintenance action on the applications unless expressly authorised by the Systems Department.

4.3 Messaging

Electronic mail: A network service that allows Employees to send and receive messages via electronic communication networks.

The rules for the use of e-mail are detailed below:

Professional use	✓ The use of e-mail should be primarily and exclusively for business purposes.
Bulk e-mails	✓ The sending of bulk e-mails for purposes unrelated to the proper performance of the Employee's duties is prohibited.
Attached information	✓ Prior to downloading any attached information received by e-mail, the Employee shall check, with due care and diligence, that the source is not malicious. In case of doubt, he/she shall consult directly with the Cybersecurity Department.
Prohibited actions	✓ Accessing or using another Employee's email account without authorisation. ✓ Attempting to read, delete, copy or modify the e-mail messages or files of other Employees. Without prejudice to the employment consequences of such conduct, such actions may constitute an offence against privacy under Article 197 of the Penal Code. ✓ Pretending to belong to a company outside Grupo IGNIS for any reason. ✓ Initiating or participating in the dissemination of chain letters or similar actions. ✓ Communicate with suppliers through private mailboxes for professional purposes related to Grupo IGNIS. ✓ Using e-mail for purposes unrelated to the Employee's duties. ✓ Sending or soliciting messages, files or materials containing sexually explicit, discriminatory, offensive, defamatory, threatening or insulting content to any person. ✓ Sending or requesting messages that include audiovisual, musical, multimedia or any other type of content which, not being related to the Employee's duties, may hinder traffic on the corporate network. ✓ Fraudulently forwarding incoming or outgoing e-mails (or their attachments) to external e-mail accounts or using the blind carbon copy (COO) system to forward the information to external accounts. ✓ Sending emails of a professional nature or related to Grupo IGNIS from the user's private email addresses (*hotmail, gmail* or other accounts). ✓ Making it difficult for Grupo IGNIS to back up a corporate mailbox.

	✓ Sending confidential Grupo IGNIS documentation to third parties to whom it is not properly justified.

The above rules, with the necessary adaptations, apply to any other digital communication system, especially messaging or similar services.

4.4 Internet:

Internet: A worldwide computer network that uses the telephone line to transmit information.

The rules for Internet use are detailed below:

Professional and responsible use	✓ The Employee shall use the Internet on the Equipment provided by Grupo IGNIS for lawful and professional purposes. Personal use shall be exceptional. ✓ In such connections, the Employee shall not disclose information that may concern private or intimate matters that he/she does not wish to be known by third parties, given Grupo IGNIS's control powers also applicable to these connections. ✓ Private use of the corporate Internet is permitted on an occasional and exceptional basis, with the Employee assuming the possible monitoring of the activity, when it is carried out under the following conditions: • Does not interfere with the functions and tasks performed by the Employee or his or her productivity. • The Group's IT security is not compromised. • Do not consume excessive bandwidth or disrupt the use of the network by other Employees and/or applications. • Do not be abusive.
Prohibited actions	✓ Downloading and/or installing software, executable files or databases from the Internet. If necessary for the performance of their duties, Employees must request authorisation from the Systems Department to initiate the download or installation of any software, executable files or databases from the Internet that are not present by Grupo IGNIS. However, the downloading of documentation uploaded to official archives or other reliable sources shall

	not require authorisation. ✓ Sharing Grupo IGNIS confidential information via file sharing software (e.g. Wetransfer or similar), using means determined by the IT Department. The Employee shall ensure that the Group's confidential information being shared is sent in accordance with the procedures in place to preserve its confidentiality. ✓ Using any software for downloading music, films, videos and/or games or multimedia reproduction services for leisure purposes, or viewing any video and/or multimedia product in streaming mode or similar provided that it prevents the proper performance of the Employee's activity, with Grupo IGNIS having the power to limit or prohibit these uses if the Employee reduces his/her productivity or does not comply with his/her obligations. ✓ Accessing websites expressly prohibited by the Group's internal policies or which contain inappropriate content or which harbour doubts as to their legality, also avoiding websites that automatically redirect to others where it is not possible to establish any control or supervision whatsoever. It is also forbidden to attempt to modify the security parameters implemented in the Corporate Internet Network and Systems in order to gain access to such websites. ✓ Use the connection provided by Grupo IGNIS to access the Internet with any private or external device, unless expressly authorised by the Systems Department. ✓ Accessing the Internet via open public connections, e.g. public transport, hotels, hotels, shopping centres, hotels, etc.

4.5 Data networks

Data network: Infrastructure whose design enables the transmission of information through data exchange (e.g. SharePoint, company intranet, etc.).

Prohibited actions	✓ Attempting to access, read, delete, copy or modify the files of other Employees without the knowledge and consent of their author or, where applicable, of Grupo IGNIS. ✓ Attempting to access restricted areas of the computer systems of Grupo IGNIS, its Employees or third parties.

	✓ Destroying, altering, disabling or damaging the data, programs or electronic documents of the Grupo IGNIS, its Employees or third parties. ✓ Attempting to modify the privilege level of an Employee in the system. ✓ Attempting to decipher the keys, systems, encryption algorithms or any other security element involved in the telematic processes of Grupo IGNIS, its Employees or third parties. ✓ Voluntarily obstructing the access of other users to Grupo IGNIS's equipment and systems, through the massive consumption of computer and telematic resources, as well as carrying out actions that damage, interrupt or generate errors in said equipment and systems. ✓ Introducing programs, viruses, macros, applets, ActiveX controls or any other logical device or sequence of characters that cause or are likely to cause any type of alteration to computer resources. ✓ Introducing, reproducing or distributing computer programs not expressly authorised by Grupo IGNIS, or any other type of work or material whose intellectual or industrial property rights belong to third parties. ✓ Making equipment and software supplied by the Company available to unauthorised third parties. ✓ Sharing resources (files, directories, etc.) without the necessary security mechanisms available in each operating system and/or applications that guarantee the security of your computer and the network.

4.6 Social networks

Scope of application	✓ These rules apply to the use of social media: • *Corporate and personal, the* latter exclusively in cases where personal use may have significant consequences or implications for Grupo IGNIS. • Irrespective of whether the social networks have been accessed via Group equipment or the Employee's personal equipment.

Use of corporate social networks	✓ Grupo IGNIS uses its corporate social networks in accordance with the principles, values and rules reflected in its internal policies, and most particularly in its Code of Ethics and Conduct, as well as with the legislation in force. Any Employee accessing such networks must do so in accordance with these regulations. ✓ If an Employee's duties require him/her to use the corporate social network, this must be done in a responsible manner and he/she must have the appropriate authorisation to do so. Any information published on Grupo IGNIS's internal channels may not be published in external media without the authorisation of the Communications Department. ✓ Employees must never use corporate channels for their own personal communications, nor create or register an account or channel on social networks on behalf of Grupo IGNIS or any member thereof, without the corresponding prior authorisation. Only the Communications Department is authorised to open digital channels (social networks, websites, blogs, etc.) on behalf of Grupo IGNIS.
Use of personal social networks	✓ The use of the Employee's personal social networks during work time should be done with due moderation and in accordance with the rules set out in this Policy, and provided that it does not adversely affect the Employee's performance. ✓ Personal use of Social Media may not be made in breach of Grupo IGNIS policies, in particular the Code of Ethics and Conduct, Anti-Corruption Code and Harassment Prevention Protocol. ✓ No comments may be published on confidential or proprietary business aspects of Grupo IGNIS, or others that may directly or indirectly harm the Company's business, image or reputation.

4.7 Digital certificates

Electronic Certificate (or digital certificate): Digital file issued by a trusted third party (a Certification Authority) that guarantees the link between the identity of a person or entity and its public key, thus allowing the holder to be unequivocally identified.

Digital certificates of	✓ They may only be used by the Employee for the legal fulfilment of their employment obligations with the

representation and/or power of attorney of Grupo IGNIS	corresponding authorisation in accordance with the procedures in force. Such use shall be terminated, with the cancellation of these certificates, upon termination of the relationship with Grupo IGNIS as proxy of the Group or the termination of their functions as its representative.
Use of personal digital certificates	✓ Personal Digital Certificates may be used both personally and professionally, insofar as they identify the person, but not necessarily within Grupo IGNIS.

4.8 Mobile phones

Permitted personal devices	✓ Grupo IGNIS makes available to its Employees a sufficient monthly financial amount for the contracting and/or maintenance, directly with the communications service provider, of an individual mobile telephone line and terminal for strictly professional use. For this purpose, the Employee shall make available to Grupo IGNIS a telephone line for professional purposes, either his own or a specifically contracted mobile line (hereinafter, any mobile line for professional use shall be referred to as a **"Mobile Device"**). ✓ In order to make professional use of the Mobile Device, the Employee shall be obliged to install the Company Portal application. ✓ Grupo IGNIS reserves the right to restrict or disable any service and access to corporate information from the Mobile Device without prior notice, and the Systems team may require the Employee to install software and/or an application in order to comply with its duty of surveillance and supervision, including access, insofar as this is done within the framework permitted by the applicable regulations and in accordance with criteria of proportionality, reasonableness and necessity, to the Mobile Device. ✓ If the Employee has chosen to use his or her own telephone line as a Mobile Device for professional use, Grupo IGNIS may, through the Company Portal, carry out monitoring and control actions on the same with regard exclusively to its professional use and applications. ✓

Rules of use	✓ The use of the Mobile Device by Employees shall be governed by the following rules of use: • Correctly configure the security settings of the device. • Keep the operating system and all applications properly updated. • Restrict third-party applications installed on the device as much as possible. These applications have a risk in that they may include malware that can be installed on the device, making the device vulnerable, including the network to which it is connected. • Set up automatic locking of the device after a short period of inactivity. Unlocking must be done by password, unlock pattern or biometric means. • Avoid, as far as possible, the use of public wireless networks or shared use networks (internet cafés, hotels, airports, tethering points issued by other devices, among others) in order to avoid theft or loss of information on networks considered technically insecure, preferably when handling corporate information. • In the event of loss or theft of the Mobile Device, the Employee shall follow the same procedure as outlined in this Policy for the loss or theft of Equipment. ✓ Grupo IGNIS Employees shall not be obliged to participate and/or belong to professional communication groups in those mobile applications they use for personal communication (e.g. WhatsApp groups, Telegram).

5 MONITORING AND CONTROLLING THE APPROPRIATE USE OF TECHNOLOGICAL MEDIA

With reference to Grupo IGNIS monitoring and control rights there are the following types of controls over the Employee Technology Resources:

- *Of a regular, preventive and random nature*, aimed at identifying any use of those means contrary to the rules set out in this Policy, and in particular, violations of fundamental rights of individuals or obligations that may jeopardise the security and assets of Grupo IGNIS.

- *Of an investigative and specific nature*, when Grupo IGNIS has indications that a user or group of users are engaging in conduct or acts contrary to the criteria set out in this Policy.

In addition to the above controls, access to the Technology Resources may also be granted in the following cases:

- *When any type of* IT *problem or incident occurs*, whether at software or hardware level, the solution of which requires such access or control.
- *Carrying out maintenance operations*, configuration, installation of new applications, etc., that Grupo IGNIS deems appropriate for the purpose of the tools and services regulated in this Policy.
- *On the occasion of the application of data protection regulations* and, specifically, with the application of the security measures that may be defined by Grupo IGNIS on the basis of the risk analysis.

The monitoring and control powers carried out at the initiative of the Systems Department or at the request of an area shall comply with the requirements of suitability, necessity, reasonableness and proportionality, and must be authorised by the appropriate persons in charge in each case.

6 SUSPENSION OR TERMINATION OF THE RELATIONSHIP WITH THE USER

The assignment of the use of the Technology Resources to the Employees for the performance of their professional duties shall only continue for the duration of the employment or business relationship, if any, with Grupo IGNIS.

From the moment the relationship is terminated for any reason whatsoever, access to these Technology Resources shall be denied. The foregoing provision may be applied in the event of the opening of contradictory proceedings for the commission of very serious misconduct by a user.

Notwithstanding the foregoing, contemporaneously or immediately prior to the termination of the relationship, the Employee may be granted access, under the supervision of the IT Department or the person delegated by the IT Department, for the purpose of deleting and/or extracting the personal information.

After the termination of the employment relationship, Grupo IGNIS shall access the Technological Medium/s and the information contained therein without limitation,

respecting the privacy of the Employee and the secrecy of communications, deleting all the Employee's personal information in the event that this has not been done.

For the sole purpose of ensuring proper business continuity, Grupo IGNIS may access the content of e-mails opened, read and sent by the Employee, respecting the legal limits of respect for the secrecy of communications and the Employee's privacy. Without prejudice to access for other legally permitted purposes for which Grupo IGNIS is authorised.

Grupo IGNIS will set up an automatic reply for a certain period of time, which may vary between 1 and 3 months, requesting the sender to forward their e-mail to the e-mail address designated by the organisation.

In the event of termination of the relationship with the Company, the Employee who is in possession of any Technology Resources will have to return them on the date of termination of the contract by complying with the return process foreseen.

In turn, the person in charge of an Employee who terminates his or her relationship with Grupo IGNIS shall be obliged to request the return of the Technology Resources.

The above rules, with the adaptations deemed necessary, may also apply to situations of suspension of the employment relationship, especially those of long duration.

7 COMPLIANCE WITH POLICY

Employees in the performance of their duties shall not only strive to do what is legally required, but also what is in accordance with the corporate social responsibility of Grupo IGNIS in order to ensure that the principles and standards set out in this Policy govern the overall operations and day-to-day running of the Company.

The Company will deploy the necessary means to ensure that all persons to whom this Policy applies act with integrity at all times, assuming the following responsibilities, without prejudice to those set out above:

- Read, know and understand the Policy, as well as all other Grupo IGNIS policies, principles and procedures aimed at developing its commitments, in order to ensure adherence to all the requirements of the Policy.

- Comply with each of the points contained in Grupo IGNIS code, policies, principles and procedures.
- Ensure that other employees affected by this Policy and other Grupo IGNIS policies, principles and procedures are committed to and comply with it.
- Demonstrate day-to-day commitment to the principles of the Policy and other Grupo IGNIS policies and procedures, and set an example to other employees.
- Avoid any situation that could lead to illegal practices or practices contrary to the basic principles of action contained in this Code of Ethics.
- Cooperate with compliance and audit bodies by providing the information requested and being true to the facts.
- Consult the *Compliance Officer* when in doubt as to how to act in accordance with the provisions of this Policy and other Grupo IGNIS policies, principles and procedures.
- Report any incident arising from knowledge or suspicion of non-compliance with this Policy and other Grupo IGNIS policies, principles and procedures.

Failure to comply with the Policy may result in legal action. In the event of a breach of the Policy, the Company and its Employees will react immediately in accordance with the framework permitted by applicable laws and regulations, taking such lawful action as may be available to them.

The response shall be proportionate to the seriousness of the facts, irrespective of the hierarchy of the persons involved.

8 QUERIES AND COMPLAINTS

Grupo IGNIS makes available for all Employees as well as of third parties the Internal Information System (hereinafter the "**Whistleblowing Channel**") for its Spanish initials) for any party interested in reporting incidents, queries, doubts or complaints regarding the breach of the commitments of this Policy as well as all other internal and external regulations applicable.

The Whistleblowing Channel is available on Grupo IGNIS corporate website for its use by all those Employees and third parties that require it.

Any Employee who is aware or has reasons to strongly suspect of a breach of this Policy or of conducts or acts contrary to the legal system shall contact through the Whistleblowing Channel with the Compliance Officer immediately.

Grupo IGNIS Whistleblowing Channel complies with the requirements and guarantees established in Law 2/2023 on the Protection of the Informant, guaranteeing:

- Confidentiality of information.
- The absence of reprisals for the informant.
- Integrity of the traceability and handling of complaints and/or queries made in good faith.

The *Compliance Officer* shall initiate an investigation in case of detection of signs of an irregularity provided for in the Policy and/or in the applicable legislation and shall notify the beginning of such investigation to the informant and if applicable, the person denounced.

9 APPROVAL AND VALIDITY OF THE POLICY

This **Policy** was approved by the Board of Directors of Grupo IGNIS on 27th December 2023.

Since its approval, the Policy has become part of Grupo IGNIS regulations and will remain in force until its cancellation, revocation or updating is approved.

The Policy will be subject to periodic review and updating processes in order to be able to adjust it to the regulations applicable at all times, to the social and labour reality and to the Company's context.

In the event of an update of the Policy, stakeholders will be informed in a timely manner through the communication mechanisms established within Grupo IGNIS.