



**CONFIDENTIALITY COMMITMENT  
FOR GRUPO FEDOLA EMPLOYEES**

GRUPO FEDOLA  
GF-JURIDICO

## **Internal Staff Documentation – Data Protection**

**EXPLORACIONES SANTONEL, S.L. v 1.0 16 June 2023**

### **CONFIDENTIALITY COMMITMENT AND SECURITY MEASURES OF GRUPO FEDOLA FOR STAFF, INTERNS, TRAINEES, AND COLLABORATORS**

The purpose of this document is to communicate the functions and obligations of staff, collaborators, volunteers, and any user with access to data for which **GRUPO FEDOLA** is the data controller, in relation to confidentiality and personal data security measures.

The current regulations on personal data protection establish, among others, the following aspects:

- **Implementing the technical and organisational measures necessary to guarantee the security required for automated files, processing centres, premises, equipment, systems, software, and persons involved in the processing of personal data.**
- **The existence of a record of processing activities containing the processing carried out by GRUPO FEDOLA and the technical and organisational measures adopted to guarantee the security of such processing.**

#### **Basic data protection information**

##### **BASIC INFORMATION ON DATA PROTECTION**

| **Data Controller** | **GRUPO FEDOLA**, comprising:

- **GRUPO FEDOLA, S.L.**
- **PREFABRICADOS TEIDE, S.L.**
- **FERRETERIA HERMANOS LÓPEZ ARVELO, S.L.U.**
- **FEDOLA, S.L.U.**
- **BROKER FEDOLA CORREDURÍA DE SEGUROS, S.L.U.**
- **PRICEMESA, S.L.U.**
- **GF-TIC, S.L.U.**
- **CAMULSE, S.L.U.**
- **OFISABEL, S.L.U.**
- **MASQUECARPAS, S.L.U.**

**GF HOTELES**, comprising:

- **EXPLORACIONES SANTONEL, S.L.**
- **FELAHOTEL, S.L.**
- **COSTA ADEJE GRAN HOTEL, S.L.**
- **ISABEL FAMILY HOTEL, S.L.U.**
- **NOELIA PLAYA, S.L.U.** |

|---|

| **Purposes** | Management of the employment/contractual relationship with the company and other related purposes, which may be consulted in the detailed information. |

| **Legal basis** | Performance of a contract, consent of the data subject, and compliance with a legal obligation. |

| **Recipients** | You authorise the transfer of your image and your full name during your relationship with **GRUPO FEDOLA**, and thereafter as long as the images continue to be used for informational purposes, for dissemination through newspapers, magazines, catalogues, posters, brochures, promotional materials, websites, and social media, for the purpose of publicising events and activities, as well as for informative purposes regarding the staff and/or collaborators of **GRUPO FEDOLA**. If you consent to the indicated transfer and processing, tick the following box  |

**GRUPO FEDOLA** carries out Corporate Social Responsibility campaigns (for example, toy collection drives) at certain times of the year, as well as negotiating and offering discounts and/or promotions for Group employees both with the Group's own companies and with third-party companies. In order to inform you and request your collaboration, we ask for your authorisation to send you such information by any electronic means. If you agree, please tick the following box

You authorise **GRUPO FEDOLA** to send by email to the following address \_\_\_\_\_ (if none is indicated, it will be sent to your Digital Identity email address) the payslip corresponding to your monthly salary, with the aim of speeding up the provision of such information. If it contains information involving special category data (health, ideology, religion, trade union membership, etc.), the sending shall be encrypted, and a key shall be provided for its decryption and viewing. Subsequently, however, employees will be provided with a corporate email account and access to a private area where documentation relating to payslips and other matters of interest to employees will be made available.

You authorise **GRUPO FEDOLA** to collect your facial biometric data for the purpose of accessing the workplace facilities through facial recognition, thereby making access more dynamic and facilitating your work.

Likewise, your data shall be disclosed to banking entities and bodies required by law.

**Rights**                      **Access, rectification, and erasure, as well as other rights, as explained in the additional information.**

**Additional Information**                      You may consult the additional and detailed information on Data Protection in this document.

**ADDITIONAL DATA PROTECTION INFORMATION**

## 1. Who is the data controller of your data?

**GRUPO FEDOLA**, comprising:

**GRUPO FEDOLA, S.L.**

**B38573192**

Edificio Olympo, C/ Candelaria, 28, 1st floor, 38002, Santa Cruz de Tenerife

Tel.: 922151499

Email: [grupofedola@grupofedola.com](mailto:grupofedola@grupofedola.com)

[www.grupofedola.com](http://www.grupofedola.com)

**PREFABRICADOS TEIDE, S.L.**

**B38597589**

Pol. Ind. Las Eras Alta, Parcela A1, 38592, Las Eras, Santa Cruz de Tenerife

922160967

[info@prefabricadosteide.com](mailto:info@prefabricadosteide.com)

[www.prefabricadosteide.com](http://www.prefabricadosteide.com)

**FERRETERIA HERMANOS LÓPEZ ARVELO, S.L.U.**

**B38402046**

Ctra. Tacoronte-Tejina, 215, 38350, Tacoronte, Santa Cruz de Tenerife

922220611

[info@comercialhermanoslopez.com](mailto:info@comercialhermanoslopez.com)

[www.comercialhermanoslopez.com](http://www.comercialhermanoslopez.com)

**FEDOLA, S.L.U.**

**B38015293**

Calle Camelias, 6, 38107, El Chorrillo, Santa Cruz de Tenerife

922614112

[www.fedola.com](http://www.fedola.com)

[pedidos@fedolafresh.com](mailto:pedidos@fedolafresh.com)

[www.fedolafresh.com](http://www.fedolafresh.com)

**BROKER FEDOLA CORREDURÍA DE SEGUROS, S.L.U.**

**B38954046**

Carretera Gral del Norte 439, La Caridad, 38340 Tacoronte, Santa Cruz de Tenerife

922536232

[brokerfedola@brokerfedola.com](mailto:brokerfedola@brokerfedola.com)

[www.brokerfedola.com](http://www.brokerfedola.com)

**OFISABEL, S.L.U.**

**B76807403**

Carretera Gral del Norte 439, La Caridad, 38340 Tacoronte, Santa Cruz de Tenerife

922570864

info@carlintenerife.com

[www.carlintenerife.com](http://www.carlintenerife.com)

**MASQUECARPAS, S.L.U.**

**B76807395**

Calle Bocatuerta 18, San Cristóbal de La Laguna, 38296

674 066 743

[www.masquecarpas.es](http://www.masquecarpas.es)

**PRICEMESA, S.L.U.**

**B38954053**

Pol. Andoriñas, Nave 1, Vía Principal Las Chafiras, 38639, Las Chafiras, San Miguel de Abona

922735155

comercial@pricemesa.com

[www.pricemesa.com](http://www.pricemesa.com)

[www.priceformes.com](http://www.priceformes.com)

**CAMULSE, S.L.U.**

**B76628072**

Avda. de Bruselas, 16, 38660, Adeje, Santa Cruz de Tenerife

922 71 67 77

[www.camulse.com](http://www.camulse.com)

[www.biospawellness.com](http://www.biospawellness.com)

**GF-TIC, S.L.U.**

**B76668854**

C.C. Aquamall, Avda. Moscú, 38, local 8, 38660, Adeje, Santa Cruz de Tenerife

822250576

info@gf-tic.com

[www.gf-tic.com](http://www.gf-tic.com)

**GF HOTELES**, comprising:

**EXPLOTACIONES SANTONEL, S.L. (GF VICTORIA \*\*\*\*\* GL)**

**B38588760**

Plaza Bischofshofen, 4, 38660 Costa Adeje, Santa Cruz de Tenerife

922747000

info@gfhoteles.com

[www.gfvictoria.com](http://www.gfvictoria.com)

**COSTA ADEJE GRAN HOTEL, S.L. (GF Gran Costa Adeje\*\*\*)\*\***

**B38555140**

Avda. Bruselas 16, 38660, Adeje, Santa Cruz de Tenerife

922719421

reservas@costaadejegranshotel.com

[www.gfhoteles.com](http://www.gfhoteles.com)

**\*\*ISABEL FAMILY HOTEL, S.L.U. (GF Isabel \*\*)**

**B38964490**

Avda. Moscú, 2, 38670, Costa Adeje, Santa Cruz de Tenerife

922715326

reservas@isabelfamilyhotel.com

[www.isabelfamilyhotel.com](http://www.isabelfamilyhotel.com)

**FELAHOTEL, S.L.U. (GF FAÑABE\*\*)\*\***

**B38489688**

Av. de Bruselas, 13, 38660 Costa Adeje, Santa Cruz de Tenerife

922 712 900

info@gfhoteles.com

[www.gfhoteles.com](http://www.gfhoteles.com)

**NOELIA PLAYA, S.L.U. (A.T. GF NOELIA\*)\*\***

**B38741013**

Avda. Hermanos Fernández Perdigón, 9, 38400, Puerto de la Cruz, Santa Cruz de Tenerife

922975154

reservas@noeliaplaya.com

[www.gfhoteles.com](http://www.gfhoteles.com)

## **2. For what purpose do we process your personal data?**

At **GRUPO FEDOLA**, we will process your personal data for the purpose of managing and maintaining the internal relationship between the company and employees, and for the following purposes:

- **Management of the employee's personnel file.**
- **Carrying out all administrative, tax, and accounting procedures necessary to comply with our contractual commitments and obligations under labour law, Social Security, occupational risk prevention, tax, and accounting regulations.**
- **Management of salary payments through a financial institution.**
- **Workplace control by monitoring the user's activity on both physical and mobile equipment and devices.**
- **Management of the company's collective insurance / pension plan.**
- **Carrying out training activities, whether subsidised or non-subsidised.**
- **Publication of your images where you have given your consent.**

- **Sending documentation and corporate notifications to your private email address.**
- **Time recording.** When the employee has authorised time recording through biometric data, such data shall be incorporated into **GRUPO FEDOLA's** information systems. In order to carry out such time recording, it is necessary to collect the following data:
  - **Biometric data**
  - **Employee code**
  - **First name and surname**
  - **Employee category**
  - **Department to which they belong**
  - **Record of working days completed**
  - **Attendance records**
  - **Daily schedules assigned to the employee**
  - **Location of the terminal used to clock in**
- **The biometric recognition system shall be carried out through clocking devices installed in the workplace in application of the authority granted by Article 20 of the Workers' Statute and with respect for the right to privacy in the employment relationship of employees (Workers' Statute Article 20 bis), and in accordance with Regulation (EU) 2016/679 of 27 April (GDPR) and Organic Law 3/2018 of 5 December (LOPDGDD).**

In this regard, **Article 20.3** establishes that the employer may “**adopt such surveillance and control measures as it deems most appropriate to verify compliance by the worker with their labour obligations and duties, while in their adoption and application showing due consideration for their human dignity and taking into account, where appropriate, the real capacity of workers with disabilities.**”

### **3. How long will we keep your personal data?**

Your personal data shall be kept for the duration of the employment relationship, and once it has ended, it shall be retained for the legally established limitation periods.

Data processed on the basis of your consent, including your images, shall be retained unless you request their erasure or withdraw the consent given.

### **4. What is the legal basis for the processing of your data?**

The legal bases that legitimise the processing of your data by **GRUPO FEDOLA**, among those set out in **Article 6.1 of the GDPR**, are:

- **Performance of a contract:** processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract (**maintenance of the employment relationship**).
- **Processing is necessary for compliance with a legal obligation:**
  - Processing of data arising from employment relationships is legitimised under labour law and occupational risk prevention regulations.
  - The entity's tax obligations, in accordance with the **General Taxation Law**.
- **The data subject gave consent** to the processing of their personal data for one or more specific purposes by ticking the authorisation boxes included in this document.
- **Article 9.2(b) of the GDPR:** "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject."
- **Royal Legislative Decree 2/2015 of 23 October**, approving the consolidated text of the **Workers' Statute Law**, and the obligation to record working time as set out in **Articles 12, 34.9 and 35**.
- **The authority granted by Article 20 of the Workers' Statute and with respect for the right to privacy in the employment relationship of employees (Workers' Statute Article 20 bis).**

#### **5. To which recipients will your data be disclosed?**

Your data shall be disclosed to the entities and organisations listed below:

- **To Grupo Fedola** for staff administrative management and internal audits
- **To banking institutions** for salary payment
- **To the Tax Administration**
- **To Social Security bodies, the Mutual Accident at Work and Occupational Disease Insurance Entity of the Social Security system**

- **To the training course management entities**, for courses you wish to attend
- **To the trade union to which you belong** for the deduction of union dues
- **To contracting companies**, where essential, in compliance with current procurement regulations
- **To other bodies required by law**

No international transfers of your personal data to a third country or international organisation are planned.

## 6. What are your rights regarding the processing of data?

You may exercise the following rights before **GRUPO FEDOLA**:

- **Access** your personal data
- **Rectify** them when they are inaccurate or incomplete
- **Request erasure or deletion** of the data when, among other reasons, they are no longer necessary for the purposes for which they were collected
- **Object** to their processing
- **Request restriction of processing** of your data when any of the conditions provided for by the regulations apply
- **Request portability** of your data in the cases provided for by the regulations
- **Prevent being subject to automated decisions**
- **Withdraw the consents granted**

To exercise these rights, the user must send a written request indicating the right they wish to exercise and attach proof of identity and a postal or electronic address for notification purposes. This request may be made to our postal address or to the email address: **fedola@dpocanarias.com**.

**GRUPO FEDOLA** must respond to the request to exercise rights within **one month** from receipt of the request. This period may be extended by **two months** where necessary, taking into account the complexity and number of requests. We will inform you of any extension within one month from receipt of the request, stating the reasons for the delay.

Likewise, data subjects have the right to lodge a complaint with the competent **Supervisory Authority (Spanish Data Protection Agency)** when they consider that **GRUPO FEDOLA** has infringed the rights granted to them by data protection regulations at [www.aepd.es](http://www.aepd.es).

With regard to the processing of health data referring exclusively to the degree of disability, or the mere declaration of disability or invalidity status of the employee or members of their family unit, when provided to **GRUPO FEDOLA**, such processing shall be limited to compliance with public duties and current legislation.

In this framework, you expressly authorise **GRUPO FEDOLA** to transfer your personal data, including those relating to the disability certificate, to the **Canary Islands Employment Service** or other public administration, for the purpose of evidencing the employment of persons with disabilities and, where appropriate, justifying the social benefits obtained.

With regard to the processing of other health data limited solely to indicating the existence or non-existence of common illness, occupational illness, work-related or non-work-related accident, as well as incapacity for work, such processing shall be limited to compliance with the obligations imposed on the company by current Social Security legislation.

## **SECURITY MEASURES AT GRUPO FEDOLA**

The following security measures are mandatory for all **GRUPO FEDOLA** staff.

### **I. Policy on the use of IT resources**

An IT resource shall be understood as any element or software made available to system users (**employee, volunteer, trainee, collaborator, etc.**) by **GRUPO FEDOLA**, whether physical (**computers, printers, mobile phones**) or virtual (**shared folders, email accounts**).

For the determination of the limits or qualifications of fundamental rights that are lawful and constitutionally admissible, the control systems established by **GRUPO FEDOLA** shall be governed by the principles determined by the Constitutional Court: **suitability test, necessity test, and proportionality test in the strict sense**. To this shall be added the safeguards and guarantees required and established by our case law.

**GRUPO FEDOLA** shall establish protocols and implement rules for the use of IT resources in order to clearly define the framework of action, responsibilities, and guarantees of all parties involved. Specific policies shall also be developed for the use of the Internet, email, and file-sharing programs, without invalidating what is specified in this policy.

Regardless of the foregoing, it is stated that the IT resources provided by **Grupo Fedola** shall be used **only for professional purposes**, and any personal use thereof is prohibited.

In addition, it is stated that the technological means provided by the company shall be used lawfully, avoiding any conduct that constitutes a breach of current legislation.

In this regard, actions aimed particularly at committing cybercrime, disclosing confidential information of the company or employees, promoting crimes of a sexual nature, committing offences of corruption of minors, forgery, damaging the company's technological equipment and software, using illicit or unlicensed software, etc., shall be particularly avoided.

IT resources are assigned and withdrawn by **GRUPO FEDOLA** at its discretion, depending on the needs of each job position and each user. Use by a user of such resources does not imply any future right to access them.

Accounts on **GRUPO FEDOLA** computers and devices are **personal and non-transferable**. To this end, the user shall be provided with one or more passwords to use the different resources, and it is their responsibility to safeguard such passwords. It is therefore prohibited to disclose the password to other persons, whether or not they belong to **GRUPO FEDOLA**. Common names, vehicle registration numbers, telephone numbers, names of relatives or friends, and derivatives of the username, such as changes in letter order or repeated letters shall be avoided.

The user must inform the person designated by **GRUPO FEDOLA** of any fraudulent use by a third party of the resources made available to them, as soon as they become aware of it.

No software, logical device, or sequence of characters that may cause any present or future alteration or damage to **GRUPO FEDOLA's** computer systems shall be introduced.

The installation of any type of software or hardware is prohibited without prior verification that the corresponding licence is available. The introduction of such software or devices shall always require prior authorisation from the system administrator.

**GRUPO FEDOLA's** databases containing personal, professional, or organisational data of users, clients, suppliers, employees, etc. are **non-public sources**. They shall strictly comply with current legislation and shall have strict security protocols, and access and use of permissions. These databases may not be used for purposes other than those for which they were created, nor by personnel without proper authorisation.

If, in the course of the employee's work, they need to provide a collaborator/supplier with sensitive company data, such disclosure must first be communicated to their immediate superior, and the legal department must be consulted as to whether a confidentiality agreement or equivalent document needs to be signed.

## II. Management of media and/or personal devices

For data security reasons, the use of personal storage media by employees, collaborators, etc. is prohibited, unless authorised by the supervisor and the system administrator (**GF TIC, S.L.U.**).

**GRUPO FEDOLA** has no control over the storage media used, so deletion of the information when the relationship with **GRUPO FEDOLA** ends is required. The owner of the device is responsible for implementing the necessary security measures to safeguard the data managed on it.

To maintain control over access to data through personal storage media/devices, the following must be specified below, not only the device used, but also the information accessed:

<b>Storage Medium/Device</b>	<b>Application Accessed</b>	<b>Data Accessed</b>
----------------------------------	---------------------------------	--------------------------

In the case of desktop computers and laptops, we recommend creating two types of user sessions: one for work-related activities and another for leisure and access by other members of the household. This prevents access to data by third parties not involved. The work session must be protected by username and password and have a password-protected screensaver activated in order to lock it during periods when the user is absent. The password used must be personal and must be changed at least once a year.

In addition, the device's operating system must be updated to its latest version and regularly scanned by antivirus software to protect it against possible malware threats.

With regard to Internet connections, it should be noted that they must be made through secure lines: the use of public networks should be avoided, since we do not know the router configurations and run the risk that passwords and information may be stolen or accessible to third parties.

It is not advisable to use personal smartphones/tablets to obtain data, but where unavoidable for operational reasons, and always when authorised, it must be borne in mind that temporary files should not be left on the device. During the transfer of documents, images, etc. to systems/server, it is advisable to **cut** the files rather than copy them, thus ensuring that no copy remains on the device.

At the end of the employment relationship, the employee shall deliver and return to **Grupo Fedola** any documentation and information owned by **Grupo Fedola**. After such delivery, they must delete from their personal devices the documentation and information owned by **Grupo Fedola** by means of a procedure with the maximum

guarantees so that recovery of the information is not possible. Any remaining information belonging to **Grupo Fedola** must be delivered to their supervisor.

Finally, employees are informed that they may be included in **WhatsApp groups** or similar instant messaging programs for work-related or non-work-related communications. If they do not wish to be included, they must notify their superior or Human Resources in writing.

### **III. Protocol for the use of email**

Email is a working tool provided by **GRUPO FEDOLA** to its staff, regardless of the legal form through which such services are provided. Therefore, such email must be used **only for professional/work-related purposes** in relation to **Grupo Fedola**.

To this end, an individual email address shall be assigned to those work positions that reasonably require its use, and **GRUPO FEDOLA** shall have the authority to organise it and determine the system to be followed.

Users shall avoid, as far as possible, providing their email address for private purposes to persons or institutions which, outside their family or circle of friends, may create a risk of mass or improper mailings. In any case, if such situations arise, they shall adopt the appropriate measures or request them from the systems managers.

Passwords are the best defence against unauthorised use of an email account. Users must not provide them to others, write them down in a visible place, or store them in media not authorised by the company. An easily-deduced password shall not be used, and the user shall block access to the email account if absent from the workstation during the working day.

Subscription to mailing lists or other email subscription services is only admissible if related to the user's role at **GRUPO FEDOLA**.

Users shall endeavour to avoid excessive storage of emails, particularly those with large attached documents.

In order to avoid overloading the computer system responsible for the email service, **GRUPO FEDOLA** reserves the right to establish space quotas available for each email account, and the sending and/or receipt of messages may be automatically restricted if the established limit is exceeded. Likewise, **GRUPO FEDOLA** reserves the right to establish a size limit for individual messages processed, and delivery or receipt of those exceeding this limit may be cancelled.

As a general criterion, and insofar as the email indicates that it originates from **GRUPO FEDOLA**, any content contrary to the ethical principles commonly accepted by society, opposed to public order, or infringing the fundamental rights of the person shall be avoided.

Except for the exceptions contemplated in the following section, the use of another user's email is prohibited, in order to avoid, due to the resulting confusion, any type of damage to either party or to **GRUPO FEDOLA**.

Since it is generally accepted that the introduction of viruses into computer systems occurs mainly through email, all system users have the obligation to exercise the utmost diligence in order to avoid this type of problem. In any doubtful or risky situation regarding the possible introduction of viruses, users must contact the system administrator and follow the instructions provided by them.

When the email contains **special category data (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, and data relating to criminal convictions and offences)**, it may not be forwarded without authorisation from the employee's immediate superior, and in any case its content must be encrypted and the password provided by other means.

Failure to comply with these rules shall result in the restrictions that **GRUPO FEDOLA** deems appropriate and, where applicable, the disciplinary measures that may be appropriate.

#### **IV. Internet**

Unnecessary network traffic unrelated to the activity carried out by the user at **GRUPO FEDOLA** and which may interfere with other users' ability to use network resources effectively or diminish such resources must be minimised. The network must not be overloaded with excessive data, nor must the institution's IT resources be misused.

A series of prohibitions is established below:

- **The voluntary and conscious viewing or downloading, creation, distribution, or exchange of offensive or obscene content, including pornographic material, as well as any other content that promotes, praises, or incites discrimination based on race, sex and/or sexual preference, nationality or xenophobia, age, marital status, sexual orientation, or disability.**
- **The promotion or incitement of activities or attitudes that favour, protect, or glorify discrimination based on race, sexuality or sexual choice/orientation, opinion or politics, as well as any discrimination based on nationality, age, gender, marital status, or disability.**
- **The voluntary and conscious access to websites, intranets, forums, chats, etc., containing threatening or violent material.**

- **As a general rule, mass mailings may not be carried out unless authorised by GRUPO FEDOLA.**
- **Failure to comply with these rules shall result in the restrictions that GRUPO FEDOLA deems appropriate and, where applicable, the disciplinary measures that may be appropriate.**

It is also established as an obligation that registration in systems of any kind, including websites, must be carried out with a company account, a secure password, and, where possible, **two-factor authentication**. If the system requests a second account for recovery purposes, this must also be a company account. Identity theft resulting from failure to follow these recommendations shall be the employee's responsibility.

#### **V. File-sharing programs**

The risks arising from the use of **peer-to-peer (P2P) network programs** and any other variation intended for file sharing between individuals, whether free, paid, or using any other system, mean that **GRUPO FEDOLA expressly prohibits this type of software**.

Through such programs, viruses, trojans, worms, or back doors may be introduced into **GRUPO FEDOLA's** systems, sabotaging, overloading, or rendering useless the network or the information owned by **GRUPO FEDOLA** or any of its employees, etc.

Certain file-sharing programs between individuals may expose the full contents of the hard drives of the computers on which they are installed, jeopardising not only the information owned by **GRUPO FEDOLA** but also the personal data of users.

#### **VI. Video surveillance**

**GRUPO FEDOLA** is equipped with surveillance cameras installed visibly at the main entrances, passageways, and common areas where work is carried out, for the purpose of monitoring and controlling access.

Likewise, the images captured by the camera system may be used for monitoring work activity, time recording, and checking the entry and exit of staff, and may lead to the imposition of disciplinary sanctions for breaches of the employee's labour obligations and prohibitions, or for the commission of any offence by the employee related to their job (**theft, larceny, etc.**).

#### **VII. Monitoring**

**GRUPO FEDOLA** shall determine the process by which the use of IT resources by users is periodically monitored and controlled, in order to ensure compliance with the **Code of Conduct** and current legislation.

The monitoring established is a measure to guarantee the security and integrity of communications and of the services provided through the same. It may also make it possible to detect unauthorised or prohibited activities by system users.

Certain software programs may be installed on users' computers to make such monitoring possible, and it is prohibited to install any program or software application on the computers assigned to users that does not comply with current legislation. The monitoring of these activities shall always be carried out while guaranteeing, on the one hand, the privacy and secrecy of users' communications and, on the other hand, the security and integrity of the system.

## **VIII. Audits**

An audit is a specific and individual review of a computer, including all types of information. An audit shall only be carried out when **GRUPO FEDOLA** has express knowledge or well-founded indications that acts contrary to the **Code of Conduct**, this Protocol, and the use policies approved by **GRUPO FEDOLA** at any given time may be being committed from that computer.

The audit must be an appropriate means of achieving a legitimate purpose, and there must be no alternative way that is more respectful of the employee's rights to achieve that purpose. In all cases, access must be proportionate and limited to what is related to the object of the search.

The purpose of the audit shall be to verify the activity carried out on the computer by the user.

## **IX. IT media and documentation**

The use of information media owned by **GRUPO FEDOLA** must be for the performance of work-related activities and not for private purposes. IT media includes CDs, USB drives, and any other optical, magnetic, solid-state, or other media that **GRUPO FEDOLA** makes available to users or may make available in the future.

The installation of software not previously authorised by **GRUPO FEDOLA** is not permitted. This includes toolbars, translators, multimedia players, individual codecs or codec packs, instant messaging, and other programs, whether freeware, shareware, or payware. Any other program must be evaluated and approved by **GRUPO FEDOLA** before installation is authorised.

Any medium or document received at **GRUPO FEDOLA** must be registered, following the procedure established in **GRUPO FEDOLA's** security policies. Once processed, the medium received must be completely erased. If, for justified reasons, the received medium is to be kept, it must be inventoried, following the rules described in **GRUPO FEDOLA's** security policies.

The removal of media, documents, and personal computers outside the organisation requires authorisation. The procedure for obtaining such authorisation is described in **GRUPO FEDOLA's** security policies.

Other relevant aspects to be taken into account are the following:

- **When documents containing personal data are not in the storage devices intended for their preservation because they are under review or being processed, the person responsible for them must safeguard them and prevent unauthorised access at all times.**
- **Any security incident must be reported, following the instructions set out in the security policies.**
- **All temporary files that users keep on their personal computers must be deleted once they are no longer necessary.**
- **All documents containing personal data that are not to be archived must be destroyed following the procedure described in the security policies, once the purpose for which they were created has ended.**
- **The making of copies or reproductions of documents may only be carried out under the control of authorised personnel.**
- **Discarded copies or reproductions must be destroyed in such a way as to prevent access to or subsequent recovery of the information contained therein, for example, by shredding.**
- **Whenever physical transfer of documentation takes place, measures must be adopted to prevent access to or manipulation of the information being transferred.**
- **When accessing documents containing especially sensitive information, the employee shall use the means made available by GRUPO FEDOLA to carry out the record allowing identification of who has accessed the documents.**

#### **X. Right to digital disconnection**

In compliance with current regulations, **GRUPO FEDOLA** recognises and reminds employees of their **right to digital disconnection**.

The right to digital disconnection implies that every employee has the right to:

- **NOT answer company calls outside working hours.**
- **NOT connect to company email outside working hours.**

- **NOT use company digital devices or other digital platforms that are work tools of the company outside working hours and, in general, NOT work outside working hours unless otherwise agreed.**

The right to digital disconnection shall be exercised in accordance with the provisions of the company's digital disconnection policy, available on the website enabled for this purpose by **Grupo Fedola**.

#### **XI. Delivery of PPE/Uniforms**

**Grupo Fedola** shall deliver the relevant **PPE/uniforms** for each work position where necessary. For this purpose, the employee shall sign the corresponding receipt.

The **PPE/uniforms** must be used exclusively to perform work obligations in relation to **Grupo Fedola**.

At the end of the employment relationship, such **PPE/uniforms** must be returned by the employee in a normal state of preservation, taking into account wear and tear due to ordinary use.

#### **XII. Geolocation**

By means of this document, you are informed that company vehicles may be fitted with **GPS geolocation systems**, the purpose of which is to locate the company vehicle at all times for all relevant purposes. Such means shall be adopted with respect for the right to privacy in the employment relationship of employees (**Workers' Statute Article 20 bis**), and in accordance with **Regulation (EU) 2016/679 of 27 April (GDPR)** and **Organic Law 3/2018 of 5 December (LOPDGDD)**.

You are also informed that certain time-recording software may be used, such as attendance control software, commonly referred to as **working time clocking software**, which may include geolocation features.

#### **XIII. Anti-corruption**

Employees are informed that the company has an **anti-corruption policy** whose objective is to prevent offences such as **illegal financing of political parties, corruption between private individuals, corruption involving public officials, bribery, influence peddling, misappropriation, terrorism, etc.** This policy is available on the company website.

In this regard, all employees must avoid any conduct that constitutes a breach of the anti-corruption laws and protocols in force at any given time. If an employee detects such conduct, they must immediately inform their superior so that the appropriate measures may be adopted.

Employees also have at their disposal a **whistleblowing channel** to report irregular conduct linked to **Grupo Fedola's** activities, with full confidentiality ensured. Information on this whistleblowing channel is available on **Grupo Fedola's** website.

#### **XIV. Code of Conduct Decalogue and Code of Ethics**

**Grupo Fedola** has established a **decalogue of conduct** that has been informed and communicated to all its employees and is available on the **Grupo Fedola** website. This decalogue must be respected at all times during employees' presence at their workplace. Likewise, the **Grupo Fedola Code of Ethics** is available on the website.

#### **XV. Termination of the User's Relationship with GRUPO FEDOLA**

At the end of the relationship linking the user to **GRUPO FEDOLA** (**regardless of the nature of that relationship**), unless expressly and justifiably indicated otherwise, the entire contents of the user's equipment shall be presumed to be **non-personal in nature**, and **GRUPO FEDOLA** shall be free to review or delete them.

Under no circumstances shall **GRUPO FEDOLA** incur liability or have any obligation to communicate the contents of files located on the hard drive or the hardware or software installed, unless the user has expressly and justifiably given prior notice to that effect.

#### **XVI. Confidentiality**

The undersigned, **Mr./Ms.** \_\_\_\_\_, holder of **ID/NIE** \_\_\_\_\_, undertakes to:

1. Not disclose to any person outside **GRUPO FEDOLA**, without its consent, information to which they have had access in the performance of their duties within the entity, except where this is necessary in order to comply properly with obligations imposed on the undersigned or on **GRUPO FEDOLA** by applicable laws or regulations, or where required by lawful order of the competent authority. In the event that they use the data to which they have had access for a purpose other than those received from **GRUPO FEDOLA**, they shall also be considered a data controller, and shall be liable before the competent Supervisory Authority, or before any third party, for the infringements that may have been committed and/or for compliance with current personal data protection legislation.
2. Use the information referred to in the preceding section only in the manner required for the performance of their duties at **GRUPO FEDOLA**, and not dispose of it in any other way or for any other purpose.
3. Not use in any way any other information they may have obtained that is not necessary for the performance of their duties at **GRUPO FEDOLA**.

4. Comply, in the performance of their duties at **GRUPO FEDOLA**, with current national and European Union regulations relating to the protection of personal data.
5. Once the relationship linking them to **Grupo Fedola** has ended, or in the event of its termination, they must return the devices provided by the entity, as well as the documentation and/or media assigned to them. It is prohibited to delete company information from company devices. Furthermore, if during the relationship with **Grupo Fedola** they kept information, data, and/or documents on personal devices such as a mobile phone, laptop, or PC, they must proceed to destroy all the information retained.
6. Comply with the above commitments even after the relationship linking them to **GRUPO FEDOLA** has ended, for any reason.

Below are the portable devices supplied to you by **GRUPO FEDOLA**:

<b>MEDIUM</b>	<b>REFERENCE</b>
---------------	------------------

Company Phone	Mobile
------------------	--------

Pendrive

Laptop

Others:

Likewise, it is reminded that the user shall be liable towards **GRUPO FEDOLA** and third parties for any damage that may arise for either as a result of breach of the foregoing commitments, and shall indemnify **GRUPO FEDOLA** for any compensation, sanctions, or claims it may be obliged to pay as a consequence of such breach.

For any clarification in this regard, you may contact the **Data Protection Officer** in person.

In \_\_\_\_\_ on the \_\_\_ day of \_\_\_\_\_ 20\_\_

**Signature**