ETHICAL REGULATIONS AND CODE OF CONDUCT OF HOTELS VIVA

Published and regularly updated on the employee portal: www.portalpersonas.hotelsviva.com

ETHICAL REGULATIONS AND CODE OF CONDUCT

The management of Hotels Viva has drawn up these internal regulations to bring together a set of rules designed to help you better understand your rights and responsibilities in the workplace. The following areas are specifically addressed:

- **Policy and protocol for the prevention of sexual and moral harassment in the workplace.**
- **Specific rules of conduct during working hours.**
- **Anti-bribery and gifts policy.**
- **Rules on working hours and timekeeping.**
- **Standards, information, rights and obligations concerning personal data.**
- **Use of computers, internet, social media and email.**

Protocol for the prevention of sexual and moral harassment

Introduction
First and foremost, we would like to highlight Hotels Viva's strong commitment to preventing and eradicating all forms of sexual or gender-based harassment, as well as harassment based on racial or ethnic origin, religion or beliefs, disability, age, sexual orientation or gender. To this end, the following is set out:
This protocol comprises a Code of Conduct and a Procedure Protocol. The aim of the Code of Conduct is to promote policies and practices that foster a workplace free from sexual and moral harassment. The Procedure Protocol, meanwhile, sets out the steps to be followed should any cases of sexual or moral harassment arise.

Definition of sexual harassment
As set out in Organic Law 3/2007, sexual harassment is defined as any verbal or physical conduct of a sexual nature that is intended to, or has the effect of, undermining a person's dignity, particularly when it creates an intimidating, degrading or offensive environment.

Definition of moral harassment
Psychological harassment at work, whether between colleagues or between superiors and subordinates, whereby the affected individual is subjected to systematic and sustained attacks intended to humiliate them by imposing situations that seriously undermine their dignity.

1. Code of conduct
The company's management expresses its concern and commitment to preventing and addressing instances of harassment, and accordingly affirms its wish for all employees to be treated with dignity, without allowing or tolerating sexual or moral harassment in the workplace.
All employees share the responsibility of helping to create a working environment in which everyone's dignity is respected. **It is the clear and unavoidable duty of all company managers to act proactively in preventing, identifying and addressing such behaviour, and the management is firmly committed to taking decisive action against any conduct that violates the privacy and dignity of either women or men through such offences.**
Employees have the right to file a complaint if harassment occurs. Any such complaint will be treated seriously, promptly and in confidence. Complaints must include a description of the incidents and should be submitted, at the employee's discretion, to a member of the human resources department, their department head or the hotel director. If the employee so wishes, the matter may also be brought to the attention of the workers' legal representatives, who will then participate in the handling of the information-gathering process.

Article 54.2 (g) of the Workers' Statute defines as a serious breach of contract: "Harassment on the grounds of racial or ethnic origin, religion or beliefs, disability, age or sexual orientation and sexual or gender-based harassment of the employer or of individuals working at the company." It further establishes that such a breach constitutes grounds for disciplinary dismissal.
Article 40.12 of the National Labour Agreement for the Hospitality Sector likewise classifies the conduct described above as a very serious offence and sets out penalties ranging from suspension from work and pay for sixteen to sixty days to disciplinary dismissal.

Article 40.13 of the same agreement also defines as a very serious offence: “Moral harassment, sexual harassment and gender-based harassment, as well as harassment based on racial or ethnic origin, religion or beliefs, disability, age, sexual orientation or gender, against individuals working at the company.”

2. Procedure protocol

A) Informal procedure

As, in most cases, the primary aim is simply to stop the unwanted behaviour, it is advisable to first consider an informal approach. As an unofficial step, this involves clearly explaining to the person displaying the unwanted conduct that such behaviour is unwelcome, offensive or uncomfortable, and that it interferes with their work, with the aim of putting an end to it. This explanation may take place privately between the two employees or, at the request of the affected employee, in the presence of the department head, the hotel director, a member of the human resources department or a workers’ representative.
This unofficial step may also be carried out without the presence of the employee, if they so wish, by a person of their choosing: a workers’ representative, the department head, the hotel director or a member of the company’s human resources team.

B) Formal procedure

The formal procedure begins with the submission of a complaint, including a list of incidents compiled by the employee affected by the sexual or moral harassment, with as much detail as possible. The complaint should be addressed, at the employee’s discretion, to either a member of the human resources department or the hotel director. If the employee so wishes, a copy may also be forwarded to the workers’ legal representatives.
The complaint will immediately trigger the opening of an information-gathering procedure aimed at clarifying the facts, during which all involved parties will be heard, including the workers’ legal representatives, if any are present at the workplace.
Following this, any measures deemed necessary to determine the accuracy of the reported events will be taken.
During the course of the procedure, the complainant or the person accused may, if they wish and where feasible, request a change of post until a decision has been reached.
The involvement of the workers’ legal representatives, any witnesses and all other participants must be handled with the utmost confidentiality, as the matter directly concerns the privacy and reputation of those involved. Due respect must be shown to both the complainant and the person against whom the complaint has been made.
If sexual harassment is confirmed, the penalties set out in Articles 40.12 and 40.13 of the National Labour Agreement for the Hospitality Sector will apply.
If the facts cannot be confirmed and no disciplinary action is therefore taken, the complainant must under no circumstances be subject to retaliation. On the contrary, the situation will be monitored with particular care to ensure that no harassment occurs.
Wherever possible, efforts will also be made to organise work in a way that avoids continuous contact between the affected employees.

Specific rules of conduct

Employees must comply with the instructions issued by the company’s management or by any person to whom management has delegated authority. In particular, they must:

- Maintain good personal hygiene and ensure their work uniform is kept in proper condition, especially in customer-facing roles. The name badge must always be worn in a clearly visible position.
- Use hotel facilities responsibly and help keep them in a clean and hygienic state at all times.

- Treat all colleagues with respect, always using an appropriate tone and manner when communicating. Raising one's voice is strictly prohibited in any area of the premises.
- Enter and leave the hotel only with the company-issued handbag.
- The unauthorised appropriation of drinks, food, cleaning products or any other items – whether belonging to the hotel or to guests – is strictly forbidden.
- Any lost property found by an employee must be handed in to the department head.
- Smoking is permitted only in designated areas and during breaks agreed with the respective department heads, with **proper registration in the timekeeping system.** During the COVID-19 health emergency, or in similar situations, smoking is strictly prohibited anywhere on the premises, including outdoor areas.
- Comply with all occupational risk prevention measures.
- Comply with all measures established for the prevention of COVID-19 in the event of an emergency.
- Refrain from consuming alcohol on company premises, whether during or outside working hours, unless expressly authorised by company management. The storage, possession or solicitation of any illegal drugs on or around company premises is likewise strictly prohibited.
- Refrain from using mobile phones during working hours, unless expressly authorised by management.
- Refrain from posting any comments or images on social media related to the company that may harm its image or reputation, or that of its staff or guests.

Anti-bribery and gifts policy

We comply with all laws that prohibit bribery and do not make promises or offer favours in exchange for commercial advantage.

As Hotels Viva may be held accountable for any unlawful actions carried out by third parties working on our behalf, we exercise due diligence when engaging and supervising all third parties.

Never use or offer Hotels Viva's funds, assets, services or facilities to improperly influence a business decision.

• We do not offer to go beyond the scope of our current work in the hope of securing additional business.
• When acting on behalf of third parties, we ensure they are familiar with Hotels Viva's anti-bribery rules and monitor their actions closely.
• We carry out and record all payments and transactions accurately and honestly, and we never attempt to conceal the true purpose of any expense.
• We compete fairly by providing our guests with the best possible experience.
• We comply with competition laws designed to protect consumers and ensure a free and open market. We fully respect these laws and never attempt to restrict or distort competition.
• We do not enter into agreements (whether in person, in writing, formally or informally) with competitors that could limit competition.
• We act fairly with all Hotels Viva suppliers.
• We do not misrepresent facts when negotiating on behalf of Hotels Viva.

Working hours and timekeeping

At locations where an electronic timekeeping system is in use, the following rules must be observed:

- You must use the timekeeping device closest to your workstation.
- You must clock in and out, as well as record breaks, immediately before starting and immediately after finishing work.

In other words, you must NOT record the start of your shift upon arriving at the hotel, or the end of your shift when leaving. You MUST use the nearest timekeeping device just before starting and just after finishing your actual work.

- Use of the timekeeping device is mandatory. Failure to use it, or improper use, may be treated as a disciplinary offence.
- Any issues (such as forgetting to clock in/out, the device not recognising you or system errors) must be reported to the department head.
- The data recorded by the system may be used as evidence of absence, lateness or early departure.

However, simply clocking in outside scheduled hours does not in itself indicate that overtime has been worked. All overtime must be approved in advance by the hotel or workplace director.

Protection of personal data

1. Information

This privacy policy applies to the processing of HR-related data at HOTELS VIVA & RESORTS. Please read it carefully, as it contains important information about how your personal data is handled, the rights granted to you under current data protection laws and your corresponding responsibilities.

We reserve the right to update this information at any time, either as a result of business decisions or to comply with changes in legislation or case law. If you have any questions or require further clarification regarding the data protection information provided here or your rights, you may contact us using the channels indicated below.

1. Who is responsible for processing your data?

The data controller is the HOTELS VIVA & RESORTS company with which you have an employment or contractual relationship (hereinafter, the COMPANY). HR data from all HOTELS VIVA & RESORTS companies is consolidated at a corporate level for the purposes outlined in this policy. The entity responsible for processing this consolidated data is INVERSIONES PASCUAL, S.L., with its registered office at Calle Agustín Argüelles, 1, 07400 Alcudia, Balearic Islands, Spain (hereinafter, HOTELS VIVA & RESORTS).

If you have any questions regarding data protection, you may contact the Data Protection Officer at Calle Agustín Argüelles, 1, 07400 Alcudia, Balearic Islands, Spain, or via email at dpd@hotelsviva.com.

2. Why do we process your data and on what legal basis?

Employee data is processed for the following purposes:

2.1. HR management
2.2. Timekeeping control
2.3. Implementation of monitoring and oversight measures in the workplace
2.4. Capturing and use of images
2.5. Consolidation of HR data
– INTERNAL ADMINISTRATIVE PURPOSES
– PAYROLL MANAGEMENT
– INTERCOMPANY RECRUITMENT
– MANAGEMENT CONTROL AND BUSINESS DATA ANALYSIS

Further details on each of these purposes are provided below:

2.1. HR management

The COMPANY will process your data for the management, administration, organisation, planning and training of its human resources.

The categories of data processed by the COMPANY for this purpose include:

- Identification and contact details, such as DNI/NIE (Spanish ID document/Foreigners' ID document), full name, residence permit (where applicable), address, telephone number, email, signature, image/voice and Social

Security/Mutual Insurance number. The mobile phone number you have provided will be used to exchange operational communications via WhatsApp or any other messaging app agreed with the company.
- Personal details such as marital status, date of birth, nationality and spoken languages.
- Academic and professional background.
- Employment details.
- Financial, banking and insurance data, including your bank account and payroll information.
- Data relating to transactions involving goods and services.
- Data generated from the employment relationship, including your employment contract or any agreement governing your placement, internship or traineeship, any amendments thereto and employment records such as timekeeping logs.
- Special categories of data: We process health data where necessary to comply with our obligations under employment law, occupational risk prevention, social security or the inclusion of people with disabilities. This includes, for example, information relating to sick leave, disability status and degree of disability. We may also process trade union membership data for the purpose of collecting union dues, if you have requested this. In such cases, the processing of your trade union membership data is based on the consent you have provided, which you may withdraw at any time by contacting the HR department.

The processing of this data is necessary for the performance of your employment contract, or the agreement governing your placement, internship or traineeship, as applicable, and to ensure the COMPANY's compliance with its legal obligations in relation to employment, occupational health and safety, social security and the social inclusion of people with disabilities.

Financial data and data relating to transactions involving goods and services generated through the employment relationship will be processed for administrative and accounting purposes, as well as to comply with the COMPANY's legal obligations in the areas of accounting and taxation.

All of this data is obtained either directly from you or generated through the contractual relationship itself. The COMPANY may negotiate preferential conditions for the provision of products or services by third-party companies. Please note that we are not a party to any contractual relationships that may be established between you and these companies.

2.2. Timekeeping control

The COMPANY will process the data recorded in the working hours log in order to monitor your working time, in compliance with Article 34.9 of the Workers' Statute.

The COMPANY will also process the mathematical pattern generated from your facial scan solely for the purpose of verifying your identity when using the timekeeping system. The use of a biometric verification system is based on our legitimate interest in ensuring the fast and efficient authentication of individuals clocking in and out of work.

How has this interest been balanced against your rights and freedoms? This balancing has been carried out on the following basis:

- Article 20.3 of the Workers' Statute grants employers the right to adopt monitoring and control measures they deem appropriate to verify that employees are fulfilling their duties and obligations.
- The processing is in line with the reasonable expectations of data subjects, as this is a common practice in many companies.
- The impact on individuals' privacy is minimal, as the facial pattern is used solely for verification purposes and not for biometric identification. Furthermore, the biometric system does not store facial images, nor can such images be derived from the stored mathematical pattern.

2.3. Implementation of monitoring and oversight measures in the workplace

The COMPANY will implement measures to ensure the security of its premises, property, resources and systems. In this regard, and in accordance with Article 89.1 of Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights, you are expressly informed that images captured by video surveillance cameras installed on the COMPANY's premises – whether visible or concealed – may also be processed for the purpose of monitoring employees. This applies both to the performance of their duties and compliance with internal regulations, as well as for the investigation and prosecution of criminal offences. This processing is based on the exercise of specific rights granted to

employers under labour law and will always be carried out in accordance with the principles of proportionality and transparency.

2.4. Capturing and use of images

The COMPANY forms part of HOTELS VIVA & RESORTS, which operates a corporate website (https://www.hotelsviva.com/) and maintains a presence on social media platforms such as Instagram, X, Facebook and YouTube. During certain activities or to showcase the COMPANY's facilities, videos and/or photographs may be taken on-site in which you, as an employee, may appear. These images may be published through the channels mentioned above to inform the public about the COMPANY's services, activities or facilities. The processing and publication of your image and/or voice on the corporate website or social media channels is based on Organic Law 1/1982 of 5 May, on the protection of honour, personal and family privacy and personal image, as well as on your consent, which will be requested in each case.

2.5. Consolidation of HR data

Companies within the group share HR data with HOTELS VIVA & RESORTS for consolidation purposes. The processing of this data by HOTELS VIVA & RESORTS includes the following:

INTERNAL ADMINISTRATIVE PURPOSES

Your identifying details, job title and professional contact information will be added to the corporate directory, which is accessible to other employees. This information will also be used to create your access credentials for company systems, such as the employee portal.

HOTELS VIVA & RESORTS will additionally process this data to include you in its mailing list for internal corporate communications.

This consolidation is based on the legitimate interest recognised in Recital 48 of the GDPR, which allows the transfer of HR data between companies within the same corporate group for internal administrative purposes.

How has this interest been balanced against your rights and freedoms? In balancing this interest against your rights and freedoms, the following has been considered:

- The processing is consistent with the reasonable expectations of the data subjects, as it concerns employees of HOTELS VIVA & RESORTS companies and takes place within the context of an existing employment relationship, where such processing is necessary for its management.
- The impact on individuals' privacy is minimal, given the nature of the data involved and the specific purpose of the processing.

PAYROLL MANAGEMENT

Your bank and payroll data will be processed for the direct deposit of your salary. This processing is based on the performance of your employment contract and on a legitimate interest in facilitating efficient payroll management. In balancing this interest against your rights and freedoms, it has been determined that the processing has a minimal impact on your privacy, aligns with your reasonable expectations and does not present any significant risks.

INTERCOMPANY RECRUITMENT

With your consent, HOTELS VIVA & RESORTS will retain your employment file for potential future recruitment by other companies within the group.

Specifically, HOTELS VIVA & RESORTS may process the following data:

- Identification and contact details, such as DNI/NIE, full name, residence permit (if applicable), address, telephone number and email.
- Personal details such as marital status, date of birth, nationality and spoken languages.
- Academic and professional background.
- Employment details, including your employment history.
- Special categories of data, namely the existence and degree of any disability. This data is processed in compliance with obligations under legislation concerning the inclusion of people with disabilities.

Processing is based on the consent you provide in the employee registration form. Refusing or withdrawing consent will not affect your current position within the COMPANY. However, without it, we will be unable to contact you directly if a suitable vacancy arises in the future.
You may withdraw your consent at any time by contacting the HR department.
MANAGEMENT CONTROL AND BUSINESS DATA ANALYSIS

HOTELS VIVA & RESORTS will process data relating to personal characteristics, social circumstances, academic and professional background, employment details, financial, banking and insurance information and transactions involving goods and services – sourced from consolidated HR records – to generate reports and conduct business data analysis for business intelligence and management control purposes. These analyses and reports produce aggregated results and are used to generate statistics and forecasts that support business decision-making and help optimise processes and reduce costs.

This processing is based on HOTELS VIVA & RESORTS' legitimate interest in maintaining a consolidated view of its human resources for corporate decision-making and internal administrative purposes.

How has this interest been balanced against your rights and freedoms? In balancing this interest against your rights and freedoms, the following has been considered:

- Recital 48 of the GDPR recognises the legitimate interest in sharing HR data between companies within the same corporate group for internal administrative purposes.
- The processing is consistent with the reasonable expectations of the data subjects, as it concerns employees of companies managed by HOTELS VIVA & RESORTS and takes place within the context of an existing employment relationship.
- The impact on privacy is minimal, as technical and organisational measures have been implemented to prevent the identification of individuals by users accessing reports and analyses. These measures include the separation of systems used for business intelligence and management control from operational systems, as well as the segregation of roles between users of business intelligence tools and those responsible for system administration.

3. Who might we share your data with?

As a general rule, your data will only be shared between companies within HOTELS VIVA & RESORTS, in the situations described in the sections above, or with third parties when required by law, with your prior consent or when necessary for the performance of a contract.

Personal data required to process HR-related payments will be shared with the financial institution responsible for carrying out the relevant transfers. The direct deposit of your salary is based on the legitimate interest in facilitating payroll management. In balancing this interest against your rights and freedoms, it has been determined that the processing has a minimal impact on your privacy, aligns with your reasonable expectations (as it is a common practice) and does not present any significant risks.

To comply with legal obligations, your personal data may be disclosed to public authorities or entities, such as the labour authority, health authorities, Social Security or the Tax Agency. Where applicable, it may also be shared with the company's health and safety committee, prevention delegates, works council or staff representatives, without limitation.

4. How long will we keep your data?

In general, your data will be retained for the duration of your relationship with us and, in any case, for the time periods established by applicable law or as long as necessary to address any potential liabilities arising from the processing. We will delete your data when it is no longer necessary or relevant for the purposes for which it was collected.

Employee records will be kept for at least the minimum periods required under labour law. Records of former employees will be retained for six years from the date of termination. From that point on, a triennial review will be conducted to identify documents that no longer need to be kept, which will then be deleted. Timekeeping data will be retained for the duration of the statute of limitations for infractions, as established in the applicable collective agreement or current labour legislation, and in any case for a minimum of four years.

Data processed for publication on HOTELS VIVA & RESORTS' corporate website or social media platforms will be retained for as long as authorisation remains valid, or, in any case, for as long as the COMPANY considers necessary to fulfil the purposes for which the photos and/or videos were taken.

Images captured by video surveillance cameras will be deleted within a maximum of one month from the time of recording, unless a longer retention period is required by law – for example, to provide evidence of actions that compromise the safety or integrity of individuals, property or facilities.

Data processed by HOTELS VIVA & RESORTS for management control and business analysis purposes will be retained indefinitely, as the information is anonymised once the retention period for employee records has expired.

Documents recording your consent to the processing of your data, such as signed forms or this policy document, will be retained for the duration of the processing and for the relevant limitation periods.

5. What are your rights?

You have the right to obtain confirmation as to whether or not we are processing your personal data and, if so, to access that data. You may also request that your data be rectified if it is inaccurate or completed if it is incomplete, and request its erasure when, among other reasons, the data is no longer necessary for the purposes for which it was collected. In certain circumstances, you may request the restriction of the processing of your data. In such cases, we will only process the affected data for the establishment, exercise or defence of legal claims or for the protection of the rights of others. Under certain conditions, and for reasons relating to your particular situation, you may also object to the processing of your data. In such cases, we will cease processing the data unless we have compelling legitimate grounds that override your interests, rights and freedoms, or for the establishment, exercise or defence of legal claims. Likewise, under certain conditions, you may request the portability of your data so that it can be transmitted to another data controller.

You may withdraw any consent you have given for specific purposes at any time, without affecting the lawfulness of processing based on consent prior to its withdrawal. You also have the right to object to the adoption of automated individual decisions that produce legal effects concerning you or significantly affect you in a similar way, where this right applies under Article 22 of Regulation (EU) 2016/679.

You also have the right to lodge a complaint with the Spanish Data Protection Agency or any other competent data protection authority. You can consult the list and contact details of European data protection authorities on the European Commission website at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080.

To exercise your rights, you must send a request by post or email to the addresses indicated in the section "Who is responsible for processing your data?".

You can find more information about your rights and how to exercise them on the website of the Spanish Data Protection Agency at https://www.aepd.es.

6. What are your obligations?

You declare that the data you provide to us, now or in the future, is correct and truthful, and you undertake to inform us of any changes to it.

In the course of performing your duties, you may have access to personal data processed by the COMPANY or by companies within HOTELS VIVA & RESORTS, as well as to other information generated by their activities. Such data is subject to compliance with the applicable regulations on personal data protection.

Data is a company asset, and as such, measures have been established to ensure its quality, security, confidentiality and availability, as well as compliance with relevant legal standards.

To achieve this, you are granted access to the resources required to carry out your duties, while maintaining a level of security that protects the integrity, confidentiality and availability of information. These security measures apply regardless of the medium in which the data is stored (paper or digital), how it is processed (manually or electronically) or how it is transmitted (voice, telephone, fax, email or any other automated means).

The organisation's internal procedures, their definition and implementation, as well as working methods, templates, workflows and, in general, all elements forming part of the company's know-how, are the property of the COMPANY. Accordingly, you undertake not to reproduce, copy, distribute, publish or disclose this information to third parties, nor to use it for your own benefit, in whole or in part. You also expressly waive any rights over all documentation you produce as a result of your work for the COMPANY, in favour of the latter.

Therefore, you agree to comply with and uphold the security measures applied to processing systems, and to respect the rules for the use of the IT systems made available to you, which must always be used in accordance with the instructions provided by the COMPANY. As a general rule, the use of the organisation's IT and communication systems for personal matters or for any purpose not directly related to your job duties is prohibited. You must not use these systems to store, process or transmit content in which you have any expectation of privacy. Information stored on company systems will not, under any circumstances, be considered private or personal for privacy purposes, and the COMPANY may access such information for any necessary or appropriate monitoring.

You agree to maintain full confidentiality regarding any personal data you access or have accessed, even after the end of your relationship with the COMPANY. This duty of confidentiality and obligation of secrecy extends to all companies operating under the HOTELS VIVA & RESORTS brand.

You will find the applicable data protection policies, rules and procedures for the entities managed by HOTELS VIVA & RESORTS on the employee portal. If you do not have access to this portal, you may request login credentials from the COMPANY's HR department.

All data protection policies, rules and procedures are mandatory. You undertake to read and comply with all policies and procedures affecting your role, whether set out in this INTERNAL POLICY or in any other regulations that the COMPANY may provide now or in the future.

2. Clean desk and screen policy

Given the nature of the information handled by the company and the associated confidentiality requirements, the following guidelines must be followed:

- Clean desk policy:
  - If you leave your workstation temporarily, no confidential information should be left on your desk.
  - When someone approaches an employee's workstation, the employee must take particular care to ensure that no confidential information on the desk is visible.
  - At the end of the working day, it is recommended that all desks be cleared of any accessible information (as it could be accessed by third parties). Any documents containing personal data must be stored securely (e.g., in a locked drawer or cabinet).
- *Clean screen policy:*
  - If someone approaches and has a clear view of an employee's screen, steps must be taken to prevent them from seeing any confidential information (for example, by minimising the relevant application).
  - At the end of the working day, or when leaving the workstation temporarily, the user must log out or lock the session.
- *Other considerations:* Extra care should be taken not to leave confidential documents on photocopiers, fax machines, printers, etc. Special attention must be paid to any items left in shared or public areas.

3. Use of IT resources

3.1 General conditions

Employees are responsible for the security and protection of the resources provided to them by the COMPANY. This includes safeguarding those resources from threats such as unauthorised access, misuse, errors or omissions.

Employees must also follow the measures set out in this document and in the company's Security Policy when using and managing data in the course of their duties.

To this end, the employee declares that they:

- Understand and commit to complying with the relevant policies.
- Will protect the resources assigned to them.

- Will maintain the confidentiality and integrity of the data they access, extract from systems for local use or manage in paper format.

The COMPANY provides employees with the IT resources it deems appropriate in each case, based on the operational requirements of their assigned role.
These resources are the property of the COMPANY and, as such, may only be used for activities directly related to the employee's duties as assigned by company management. The COMPANY may also replace, withdraw, modify or disable any resource at any time, without prior notice, in accordance with operational needs and priorities.
Accordingly, you are hereby informed that the following are strictly prohibited unless expressly authorised in writing by company management or a delegated representative:

- Using company computers and IT equipment for purposes other than those defined by management.
- Using the provided internet browser and email for purposes other than those defined by management.
- Installing or modifying the operating system or any software on company devices.
- Connecting personal devices (USB drives or any other digital storage media, laptops, tablets, etc.) to company resources – including servers, computers or the corporate network.

If you are granted authorisation to connect a personal device to the corporate network, this must be done from outside the corporate network. Such access is conditional upon acceptance of the specific terms of use for the service. Acceptance of these terms must include consent to usage audits and permit the company to remotely delete corporate data in the event of device loss or termination of employment.

3.2 Web browsing

Regarding internet access provided by INVERSIONES PASCUAL S.L. or any company operating under the HOTELS VIVA brand, employees should be aware that, in carrying out their duties, they represent the company. As such, they are expected to act in a manner that reflects the ethics, professionalism, courtesy and responsibility required of all employees.
The employee further agrees to:

- Limit internet browsing strictly to websites required for the performance of their assigned tasks.
- Not use any programs to make unauthorised downloads of digital files (e.g., software, videos, music) from internet servers.
- Avoid using multimedia players that consume company bandwidth (e.g., video, radio or television streaming).
- Refrain from accessing websites that could compromise the security of the company's IT systems, such as peer-to-peer (P2P) platforms.
- Never access websites with pornographic, offensive or otherwise degrading content.
- All relevant intellectual and industrial property laws must be observed. Users must carefully verify whether any online content they intend to use is protected under these laws before using it.
- The company reserves the right to block access to websites containing prohibited content or any site that may negatively affect system performance or security, using proxies or other tools. As such, please note that internet traffic is monitored, and data obtained through such monitoring may be used as evidence of misconduct in the event of improper use.

3.3 Email use

Email is a fundamental tool in the company's daily operations, and any practice that could compromise the system's performance or proper use must be avoided.
Due to the company's organisational structure and operating needs, it is essential that some email accounts are shared between employees and that **access to any corporate email account may be required in the following circumstances**:

- By a line manager to ensure the highest possible quality of service
- In the event of medical leave taken by the account holder
- During the account holder's holiday period
- During periods of inactivity for seasonal employees

In no case is such access intended to violate the employee's privacy. This reiterates the importance of using email strictly for professional purposes.
The following email practices are expressly prohibited:

- Reading, deleting, copying or modifying messages or files addressed to other users.
- Attaching or sending chain emails or large files to multiple recipients.
- Sending messages for commercial or advertising purposes without the appropriate data protection clause.

Opening any email that appears suspicious based on the subject line or sender, as it may contain a virus.

Using the corporate email address for personal purposes or sharing it for personal use.

Employees are informed that once their employment relationship with the company ends, or in the event of a departmental change or change of role, access to their corporate email account – whether named or shared – will be granted to their replacement to ensure continuity of service at the highest possible standard.

3.4 Best practices for using email

- Avoid replying to emails unnecessarily: There is no need to respond with messages such as "thank you", "okay", etc. It is assumed that all communications are appreciated and understood unless otherwise stated. Only reply if a confirmation is requested, a specific question is asked or you believe a comment is necessary.
- Do not use the preview pane, as it increases the risk of spreading viruses.
- Do not open suspicious messages: report them to IT immediately.
- Do not send, forward or reply to emails containing sensitive data without authorisation from the hotel director or, in the case of head office, the department director.
- Use blind carbon copy (BCC) when sending a message to multiple recipients outside the company.
- Only use the "forward" function if the recipient should have access to the sender, content and the full email chain.
- Remove your signature footer if sending a private message from your professional email account.
- Clearly and concisely identify the subject of the email.
- Do not include personal data in the subject line.
- Avoid words or phrases that may trigger spam filters.
- Bear in mind that if you are expecting a response, it should come from those listed in the "To" field. Those in "CC" are included for information or oversight purposes, except when "BCC" is used to protect recipients' email addresses.

3.5 Use of internal and external communication platforms

- **This includes the intranet, Microsoft Teams, Skype and any other internal communication tools made available to employees by the company.**
- **It also includes online reputation platforms where Hotels Viva holds a registered profile, such as Booking, Expedia, Google+, HolidayCheck, Tripadvisor and Trivago.**
- **And social media profiles managed by Hotels Viva, such as Facebook, X, Instagram, Pinterest, LinkedIn and YouTube.**

Accessing these digital tools without express authorisation from company management is strictly prohibited.
These platforms must be used exclusively for professional purposes.
Company management will monitor the appropriate use of these tools, with particular attention to the following:

- Granting access to restricted information to unauthorised individuals, whether or not they are part of Hotels Viva.
- Posting comments that undermine the dignity of individuals or damage the reputation of Hotels Viva.
- Publishing personal, political or religious opinions on behalf of Hotels Viva.
- Responding disrespectfully to customer reviews or making any posts that conflict with the company's communication policy.
- Promoting third-party organisations unrelated to Hotels Viva.

3.6 Auditing and maintenance of IT resources
Hotels Viva reserves the right – and the user (employee) accepts this as a condition of using company resources – to install appropriate technical tools to review, audit, access, delete and disable any messages created, received, sent or stored on the COMPANY's email system or on any other data processing or storage device, as well as to monitor web browsing, in order to maintain system security and ensure appropriate use of resources.
To carry out audits and maintain computer equipment and installed software, the IT department management may authorise technicians within the department – or external professionals contracted for this purpose – to access user profiles. Access may be requested directly from the user, or, in their absence, by using administrator-level superuser accounts or by resetting the password.

4. Access security

The COMPANY's security system relies heavily on the proper use of passwords. For this reason, the access credentials and passwords assigned to employees are strictly confidential, personal and non-transferable. Each login consists of a user ID, which is public, and a password that must be known only to the employee.

Access credentials provided for identification – such as those used to enter company facilities, access applications, email accounts, activate the company alarm system or use other services – are for personal use only and must not be shared under any circumstances. Employees are fully responsible for any misuse of their credentials.

You are responsible for keeping your password confidential. It must never be stored in readable form, whether in digital files, on paper or in any other format where it could be accessed by others.

- If you suspect that your password has been accidentally or fraudulently discovered by an unauthorised person, you must change it immediately and notify the IT Department.
- Similarly, if you become aware of any security incident, you must report it immediately.
- Being aware of an incident and failing to report it will be considered a breach of security and, as such, a disciplinary offence.
- You must change your password regularly, using secure credentials that meet the requirements outlined in the company's Security Policy.
- When leaving your workstation, you must apply the appropriate security measures to prevent unauthorised access to data, either by locking or shutting down your device.

If any misuse is detected that compromises the COMPANY's security or violates the Security Policy or the Organic Law on Data Protection, the company may take appropriate corrective or disciplinary action and may also inspect the contents of the affected devices.

5. Data protection incidents

A data protection incident is defined as any irregularity that affects or could affect the security of information, specifically, any event that compromises its availability, integrity or confidentiality. Examples of information security incidents include:

- Breaches of data protection policies or procedures.
- Unauthorised access to restricted areas.
- Loss of confidentiality of customer or employee data.
- Unlawful disclosure of data to third parties.
- Any incident involving the organisation's assets (e.g., loss of information storage media such as USB drives or paper files).
- Requests to access customer data by individuals other than the data subject.
- Sending customer information to unauthorised companies.

Any employee may report an anomaly or suspicion that could pose, or is already posing, a threat to the security of personal data to the Security Officer as soon as possible. Incidents must be reported by email to gdpr@hotelsviva.com, providing details of the issue identified. This report must be submitted as soon as the incident occurs or as soon as you become aware of it. Being aware of an incident and failing to report it will be considered a serious breach of data security and, consequently, a disciplinary offence.

This document forms an annex to your employment contract and sets out binding rules. Failure to comply with the provisions set out here may be considered a disciplinary offence by company management, in accordance with Article 39.5 of the Fifth National Labour Agreement for the Hospitality Sector (ALEH V), which defines the following as serious offences:

"Failure to comply with the company's orders and instructions – or those of its authorised personnel – when issued in the legitimate exercise of their managerial authority, including those relating to occupational risk prevention as per the training and information provided. If such non-compliance is repeated, causes significant disruption to work or results in clear harm to the company or to other employees, it may be classified as a very serious offence."