



SOCIETAT CONCESSIONÀRIA
SON ESPASES
HOSPITAL UNIVERSITARI

Code of Conduct

Modification:

Initial drafting.
The Code is fully drafted.
Complete Update.
Update sections 9, 10 and 11.
Update 6 and inclusion: 17, 18 and 19
Update sections 4, 6, 16, 18 and 20.
Full revision of the Code, inclusion: 21.

Date:

01/09/2015
15/04/2016
27/11/2019
04/04/2022
19/12/2022
08/03/2024
07/08/2026

Review:

A
B
C
D
E
F
G



CONTENTS

1. INTRODUCTION	5
2. PURPOSE	5
3. PERSONS SUBJECT TO THE CODE.....	6
4. BODY RESPONSIBLE FOR COMPLIANCE WITH AND OVERSIGHT OF THE CODE.....	6
5. GENERAL PRINCIPLES	7
6. ETHICS CHANNEL.....	9
7. OCCUPATIONAL HEALTH AND SAFETY.....	10
8. ENVIRONMENTAL PROTECTION	11
9. ANTI-CORRUPTION POLICY.....	11
9.1. GENERAL PROHIBITIONS	12
9.2. GENERAL PRINCIPLES	12
9.3. TRAINING AND COMMITMENT	15
9.4. DISCIPLINARY FRAMEWORK.....	15
10. INFORMATION SECURITY, IT SYSTEMS AND DATA PROTECTION	16
11. UNLAWFUL ACQUISITION AND DISCLOSURE OF TRADE SECRETS.....	18
12. ACCOUNTING AND TAX OBLIGATIONS. PROTECTION OF CHUSE'S ASSETS AND PREVENTION OF MONEY LAUNDERING	20
13. INTELLECTUAL AND INDUSTRIAL PROPERTY.....	21
14. HUMAN RIGHTS POLICY.....	22
14.1. SCOPE AND APPLICATION.....	23
14.2. COMMITMENTS TO HUMAN RIGHTS	23
14.2.1. COMMITMENTS TO CHUSE EMPLOYEES	23
14.2.2. COMMITMENTS TO CUSTOMERS AND SUPPLIERS.....	27
14.2.3. COMMITMENTS TO THE COMMUNITY AND LOCAL ENVIRONMENT	27
14.3. IMPLEMENTATION, COMPLIANCE AND COMMUNICATION OF THE HUMAN RIGHTS POLICY	28
14.4. OVERSIGHT AND MONITORING SYSTEMS	28
15. RIGHT TO DISCONNECT POLICY	29
15.1. SCOPE OF APPLICATION	30
15.2. PRINCIPLES GOVERNING THE RIGHT TO DISCONNECT	30
15.3. ACTIONS AND MEASURES TO GUARANTEE EMPLOYEES' RIGHT TO DISCONNECT	31
15.4. EXCEPTIONS	34
16. CRIMINAL COMPLIANCE POLICY AND MANAGEMENT SYSTEM.....	35
17. EQUALITY POLICY	37
18. PROTOCOL FOR DEALING WITH WORKPLACE HARASSMENT, SEXUAL HARASSMENT, SEX-BASED HARASSMENT, AND HARASSMENT BASED ON SEXUAL ORIENTATION, GENDER IDENTITY OR GENDER EXPRESSION.....	39
19. COMPREHENSIVE GUARANTEE OF SEXUAL FREEDOM POLICY	40
20. POLICY GUARANTEEING THE RIGHTS OF LGTBQ+ PEOPLE.....	41
21. INFORMATION SECURITY AND DATA PROTECTION POLICY	42
22. EXAMPLES OF BREACHES OF THE CODE OF CONDUCT	44

QUICK GUIDE

A **Code of Conduct** sets out the minimum standards that must guide the conduct and behaviour of CHUSE employees. Through this Code, CHUSE communicates the ethical principles and values that form part of its corporate culture.

Who must comply with it?

CHUSE's Code of Conduct applies to its management team, all its employees regardless of their type of contract, and any collaborating person or entity acting for and on behalf of the Company.

Who is responsible for ensuring compliance?

The **Criminal and Regulatory Compliance Committee** is responsible, among other duties, for disseminating the Code and overseeing compliance with it. Any breach of the Code may result in disciplinary action.

What minimum standards of conduct does the Code set out?

1. Comply with the law

Always comply with the **legislation** and **internal rules** applicable to the activity concerned.

2. Act with moral integrity and professionalism

- Always make decisions that prioritise the Company's interests over personal or other interests.
- Act honestly and treat all people fairly and respectfully.
- Do not tolerate or engage in any violent, abusive or aggressive conduct.
- Do not discriminate under any circumstances.
- Workplace harassment is prohibited and will be addressed by the Company.
- Protect CHUSE's assets against loss, damage, misuse, theft, embezzlement, and destruction.
- Information provided on the progress of work-related activities must be truthful and accurate so as not to mislead the recipient.
- Avoid any conduct that may damage CHUSE's image or reputation.

3. Protect the confidentiality of information

Non-public information obtained in the course of one's work is **confidential** and must not be disclosed or used for personal purposes.

4. Zero tolerance for bribery, corruption and unfair competition

CHUSE competes and conducts its activities solely on the basis of quality and fair competition. CHUSE rejects any action that could be construed as an improper way of obtaining a decision in favour of CHUSE or favourable treatment for CHUSE.

5. Gifts, hospitality and favours

No gift, hospitality or favour may be accepted or offered if prohibited by law or inconsistent with normal and customary business practices or courtesies. If in doubt, consult your line manager.

6. In relation to **occupational health and safety**:

- CHUSE is committed to scrupulous compliance with the applicable legislation in order to safeguard the health and safety of its employees and to providing them with the training and resources needed to perform their duties.
- Employees must comply with occupational health and safety rules, look after their own safety and that of those around them, and use the means and resources assigned to them responsibly so that they can work safely.

7. In relation to **the environment**:

CHUSE is committed to strict compliance with applicable environmental legislation and has an environmental strategy to prevent and, where necessary, minimise the adverse effects that its activities may cause.

8. In the area of **Administration and Finance**:

- CHUSE's financial information must present a true and fair view of its economic and financial position and net assets.
- Transactions that have the purpose of tax avoidance or the falsification of accounting or financial information are prohibited.
- Payments made and receipts collected by CHUSE must comply with the applicable legislation.

9. In relation to information **security and data protection**:

Personal data protection rules must be respected, and the computer equipment and systems provided must be used in accordance with CHUSE's Internal Rules.

10. CHUSE will provide the **training necessary to ensure** that all employees have sufficient knowledge of the **Code** of Conduct and its contents.

Do you have any questions, or would you like to report a breach of the Code?

Contact the Criminal and Regulatory Compliance Body directly by emailing canaletico@chsonespases.com

You should know that:

- Your anonymity will be protected and no retaliation will be tolerated.
- Disciplinary action will be taken in response to any report made falsely or any manifestly unfounded allegation.
- The right of defence of the person concerned by the report will be respected at all times.

1. INTRODUCTION

Concesionaria Hospital Universitario Son Espases, S.A. (hereinafter, 'CHUSE') has drawn up this **Code** of Conduct (hereinafter, the '**Code**') to establish and preserve the ethical values that must guide the conduct of all its employees, collaborators and business partners, thereby ensuring that they act effectively and professionally in carrying out their activities.

2. PURPOSE

The **purpose of this Code** of Conduct is to establish the ethical principles that must govern the conduct of CHUSE employees and managers, as well as its business partners, and to define the main rules of conduct with which everyone working for the Company must comply.

These principles and rules are general in nature. Where specific regulation is considered appropriate, **internal rules** (hereinafter, the '**Internal Rules**') and **manuals** will be developed, including, among others, the following documents:

- ❖ **Internal Regulations and Procedures.**
- ❖ **Occupational Health and Safety Guide.**
- ❖ **Quality and Environmental Management Manual.**
- ❖ **Criminal Compliance Policy and Manual.**
- ❖ **Corporate Privacy Policy.**
- ❖ **Equality Plan.**
- ❖ **Policy Guaranteeing the Rights of LGTBIQ+ People.**
- ❖ **Human Rights Policy.**
- ❖ **Biodiversity Protection Policy.**
- ❖ **Information Security Policy and Manual.**

The **Code** also establishes the body responsible for the compliance function (see section 4 of this document) and determines the action to be taken when breaches of the Code are detected. Hereinafter, observance **of the Internal Rules** and, more specifically, **of the Code** will be referred to as '**Compliance**' .

3. PERSONS SUBJECT TO THE CODE

All CHUSE employees and managers (the 'Covered Persons'), as well as its business partners, are required to know and comply with the **Code**, irrespective of the type of contract governing their legal relationship or the position they hold. Covered Persons must also know and comply with the **Internal Rules** and, in particular, the manuals or guides relating to their specific activities.

Breaches of the **Code** or the **Internal Rules** will result in disciplinary sanctions in accordance with employment law, without prejudice to any administrative or criminal penalties that may also arise. Compliance with the **Code** and the **Internal Rules** forms part of the obligations inherent in the employment relationship.

Covered Persons who become aware of any breach of the **Code** or the **Internal Rules** must report it to the body responsible for Compliance: the Criminal and Regulatory Compliance Body (Órgano de Cumplimiento Penal y Normativo, hereinafter, the 'OCPN').

Although CHUSE cannot be held responsible for the conduct of third parties with which it has contractual relationships, it expects all contracted persons and companies to comply with its ethical standards and principles, particularly suppliers, agents, consultants and subcontractors. The OCPN will therefore ensure that these third parties are informed of the contents of this **Code** and that contracts entered into with them incorporate the requirements of the **Code** and, where applicable, the relevant **Internal Rules**.

4. BODY RESPONSIBLE FOR COMPLIANCE WITH AND OVERSIGHT OF THE CODE

The body responsible for compliance with and oversight of the **Code** is the Criminal and Regulatory Compliance Body (OCPN). The OCPN operates through the Compliance Committee, which comprises, at a minimum, CHUSE's General Management, Operations Management, Financial Management and Human Resources Management, together with the person responsible for Quality, the Environment and Occupational Health and Safety.

The functions and duties of this Committee are:

- Oversee compliance with the **Code** and the **Internal Rules**.
- Interpret the provisions of the **Code** and oversee their application.
- Promote awareness, dissemination and compliance with the **Code**.

- Establish appropriate communication channels through which any employee may request or provide information concerning compliance, while ensuring the confidentiality of all reports processed.
- Ensure the integrity and impartiality of any proceedings initiated, as well as the rights of anyone allegedly involved in a potential breach.
- Define the circumstances in which the scope of the **Code** must be extended to third parties entering into commercial or business relationships with CHUSE.
- Hold regular meetings to monitor compliance with the **Code** and keep minutes of those meetings.

All CHUSE departments must cooperate with the **Committee** in the performance of its Compliance function and respond to any requests it makes.

Proper implementation of the **Code** and the **Internal Rules** requires all Covered Persons to be familiar with them. To this end, the **Committee** will be responsible for disseminating and promoting awareness of the **Code**. The Human Resources Department will plan the training needed to ensure that all CHUSE employees understand the **Code** and the **Internal Rules** relevant to their activities. The Training Department will keep **records** of all training completed by employees and other Covered Persons and retain documentary evidence that the training was duly completed. The **Committee** will help ensure that all training materials are consistent with the **Code** and the **Internal Rules**.

The **Code** and the **Internal Rules** will be provided to employees when their employment relationship with CHUSE begins. Any updates will also be communicated to all employees in the organisation.

The **Code** will be reviewed periodically and subsequently approved by the **Committee**.

The **Committee** will determine the measures to be taken in the event of a breach of the **Code** or the **Internal Rules**. Where a potential infringement is detected, the **sanctions procedure** will apply as the mechanism through which CHUSE adopts the appropriate measures. The disciplinary framework applies where an internal investigation confirms that the **Code** or the **Internal Rules** have been breached. For further information, consult the procedure **on the Investigation of Breaches and Irregularities and the Sanctions Framework**.

A. GENERAL SECTION

5. GENERAL PRINCIPLES

All Covered Persons will perform their duties with integrity and in accordance with ethical principles. Conduct that is unethical cannot be justified or excused on the grounds that it benefits CHUSE. The Company rejects any benefit derived from unlawful conduct.

Covered Persons must act loyally towards the Company and avoid situations involving a conflict between CHUSE's interests and their personal interests. If a conflict of interest is unavoidable, they must inform their line manager or the Criminal and Regulatory Compliance Body and refrain from participating in any decisions affected by that conflict.

Covered Persons must maintain strict confidentiality regarding all non-public information obtained in the course of their work. This duty of confidentiality continues after their professional relationship with CHUSE ends. It also extends to any non-public information concerning third parties obtained through CHUSE's commercial or business relationships with them.

Covered Persons must perform their duties in compliance with the legislation in force (laws, regulations, circulars, etc.) and avoid any practice that is ethically unacceptable under strict standards of honesty and moral integrity.

They must also comply with CHUSE's [Internal Rules](#) and any other internal rules of conduct applicable to their activities where those rules impose stricter obligations than this **Code**.

In dealings with public authorities and third parties, whether customers or suppliers, no action may be taken that could be interpreted as an improper attempt to secure a favourable decision or preferential treatment for CHUSE. CHUSE categorically rejects all forms of corruption in both the public and private sectors.

CHUSE promotes the professional and personal development of all its employees by ensuring equal opportunities. Recruitment and internal promotion policies must not include discriminatory practices. Any discriminatory treatment of employees, suppliers or customers that violates CHUSE's ethical values will be subject to appropriate disciplinary measures.

All forms of harassment are strictly prohibited at CHUSE and will be dealt with firmly by the Company. This is set out in the [Protocol for Dealing with Workplace Harassment, Sexual Harassment, Sex-Based Harassment, and Harassment Based on Sexual Orientation, Gender Identity or Gender Expression](#), which is provided to all CHUSE employees when they join the organisation. See also section **18** of this Code.

All employees, suppliers and customers must be treated fairly and respectfully by managers, subordinates and colleagues. No abusive, hostile or offensive conduct, whether verbal or physical, will be tolerated.

All employees must provide truthful, complete, clear and timely information on the progress of activities relating

to their work. They must never knowingly provide incorrect, inaccurate or imprecise information that could mislead the recipient.

CHUSE is committed to maintaining a training policy that supports the personal and professional learning and development of its employees, with a view to achieving the highest levels of performance, quality and job satisfaction.

CHUSE provides its employees with the resources needed to perform their professional duties and undertakes to provide appropriate means to protect and safeguard those resources. All employees must use Company resources responsibly, efficiently and appropriately in their professional activities and protect them against loss, damage, theft and any unlawful or dishonest use.

Covered Persons must protect CHUSE's reputation and good standing.

6. ETHICS CHANNEL

CHUSE has an Ethics Channel through which any employee or external person who becomes aware of a breach of the **Code** or the **Internal Rules**, or of any unlawful act committed within the Company, may report it with full safeguards and without fear of retaliation.

The Ethics Channel may also be used for reports or complaints made by victims in connection with the comprehensive guarantee of sexual freedom (see section 19 of this Code). Prevention of such conduct in the digital environment is also expressly addressed.

Any CHUSE employee with reasonable grounds to believe that this **Code** or any CHUSE policy has been breached may report it through any of the following channels:

- By email to canaletico@chsonespases.com
- By submitting a written report in a sealed envelope addressed to the Criminal and Regulatory Compliance Body. The report may include:
 - The reporting person's details, if they consider it appropriate to provide them.
 - The facts that they believe constitute the breach.
- By requesting an in-person meeting, after emailing canaletico@chsonespases.com to arrange an appointment.

Reports will never be required to pass through the reporting person's line manager.

The identity of anyone who submits a report through the Ethics Channel will be kept strictly confidential.

No form of retaliation or other adverse measure will be tolerated against a CHUSE employee for reporting a suspected breach of the **Code** or the **Internal Rules**.

The Ethics Channel does not protect reports that are false or manifestly unfounded. Where there is evidence that a false report was made in bad faith, the Human Resources Department will take the appropriate disciplinary action.

When reports are handled, the right of defence of the person concerned and the **applicable data protection rules** must be respected.

For further information, consult the **Reporting Breaches and Irregularities Procedure**.

B. AREA-SPECIFIC PRINCIPLES

7. OCCUPATIONAL HEALTH AND SAFETY

CHUSE has a firm and ongoing commitment to occupational health and safety and to scrupulous compliance with all applicable **rules** in this area. This commitment is an essential value in the conduct of its activities.

CHUSE will provide all employees with the means and resources they need to perform their duties safely. Employees, in turn, must use them responsibly.

All CHUSE employees are responsible for rigorously complying with occupational health and safety rules when performing their duties and for looking after both their own safety and that of those around them.

They must also use the equipment, tools and other protective measures assigned to them properly and responsibly, particularly when carrying out hazardous activities.

They will also help foster a preventive culture by sharing their occupational health and safety knowledge with colleagues and, where applicable, with anyone under their supervision, thereby promoting compliance with best practices for preventing and protecting against occupational risks.

CHUSE is committed to maintaining certification of its occupational health and safety management system and ensuring its effectiveness through continual improvement; compliance with legal requirements and other

applicable commitments; the identification and control of occupational risks; and the integration of prevention at every level of the organisation, with the participation and consultation of employees.

8. ENVIRONMENTAL PROTECTION

CHUSE is firmly committed to environmental protection and sustainable development. To this end, it pursues an environmental management strategy based on pollution prevention, reducing the environmental impacts of its activities, using resources efficiently and continually improving its environmental performance. The organisation is also committed to maintaining certification of its environmental management system and ensuring compliance with legal requirements and the commitments it has made in this area.

In carrying out its activities, CHUSE and all its employees will act in an environmentally responsible manner, integrate sustainability criteria into the performance of their duties and contribute to the achievement of the organisation's environmental objectives.

To this end, CHUSE will guide its actions in accordance with the following principles:

- a) Conserve natural resources through the efficient and responsible use of energy, water and raw materials.
- b) Prevent pollution and reduce the environmental impacts arising from the organisation's activities.
- c) Reduce pollution and the environmental impacts arising from the organisation's activities.
- d) Train, inform and raise awareness among employees regarding environmental protection, encouraging their participation in continually improving environmental performance.
- e) Comply strictly with applicable environmental legislation and the commitments voluntarily assumed by the organisation.

9. ANTI-CORRUPTION POLICY

Through this Policy, CHUSE strictly prohibits all forms of bribery involving authorities, public officials, managers or employees of national or international public-sector companies or bodies, as well as third parties with which the Company has any form of relationship. This **Policy** therefore establishes a regulatory framework to prevent and detect corruption and bribery in CHUSE's activities and to promote full compliance by members of the organisation with anti-corruption and anti-bribery legislation. Through its Criminal Compliance Management System, CHUSE has

established measures to mitigate the risk of offences involving corruption in business, bribery and/or trading in influence.

9.1. GENERAL PROHIBITIONS

CHUSE expressly prohibits the following conduct:

- Any form of bribery involving authorities, public officials, managers or employees of national or international public-sector companies or bodies, or third parties with which the Company has any form of relationship, whether a public body or a private party, for the purpose of obtaining an improper advantage.

Accordingly, it is strictly prohibited to make, promise or offer any payment to authorities, public officials, managers or employees of national or international public- or private-sector companies or bodies, whether directly or indirectly through agents, suppliers, advisers or any other intermediaries.

- Obtaining improper advantages by exploiting personal relationships with authorities, public officials or any other private party.

CHUSE requires all decisions made by employees who have dealings with public authorities to comply strictly with the applicable law and the [rules](#) in force.

9.2. GENERAL PRINCIPLES

GIFTS AND HOSPITALITY

CHUSE prohibits members of its organisation from giving or accepting gifts, hospitality or favours in the course of their activities. Exceptionally, gifts or hospitality may be given or received provided that they are not prohibited by law, are consistent with generally accepted normal and customary business practices or courtesies, and are always of symbolic or negligible financial value.

If in doubt, do not give or accept the gift or hospitality and, where appropriate, consult your line manager.

FACILITATION PAYMENTS

Facilitation payments are strictly prohibited under this **Policy**. These are small payments made to public officials to expedite or facilitate the performance of their duties, for example access to public services, the obtaining of ordinary licences or business permits, or the completion of administrative procedures.

Any activity that could lead to a facilitation payment being made or accepted by or on behalf of CHUSE must be avoided.

CHARITABLE DONATIONS

Charitable contributions must meet the following criteria:

- They must be made to reputable and reliable charities that, preferably, are not newly established.
- No donation may be offered or made without the Compliance Committee's prior written assessment.
- Charitable contributions must be made openly and transparently.

This Policy recognises the right of members of the organisation to make charitable donations in a personal capacity. Such donations are permitted provided that it is entirely clear that the donor is not representing the Company and that no Company resources are used.

POLITICAL CONTRIBUTIONS

Political contributions are strictly prohibited.

This **Policy** recognises the right of members of the organisation to make political contributions in a personal capacity. Such contributions are permitted provided that it is entirely clear that the person making the contribution is not representing the organisation and that no organisational resources are used.

SPONSORSHIP ACTIVITIES

Sponsorship activities must be reasonable, undertaken in good faith or directly related to the promotion, demonstration or explanation of the Company's facilities, plans, assets or services.

Sponsorship activities must respect the following rules:

- Sponsorship activities must be subject to the Compliance Committee's prior written assessment.
- Partner organisations entering into sponsorship agreements must be established, reliable and of excellent reputation.
- Sponsorships must be offered in an open and transparent manner.

SUPPLIERS, ADVISERS AND BUSINESS PARTNERS

The engagement of suppliers, advisers and business partners in operations or transactions involving in any way a national or foreign public authority, body or public- or private-sector company must meet the strictest due diligence requirements.

To this end, reputable, first-rate firms will be used as suppliers, advisers and business partners wherever possible.

Due diligence mechanisms will be established to obtain the fullest possible understanding of prospective suppliers, advisers and business partners, enabling the most suitable parties to be engaged to perform their activities ethically and without causing financial loss or reputational risk to CHUSE.

Suppliers, advisers and business partners will be informed of all anti-corruption prohibitions established by CHUSE, and this will be duly documented. They must confirm their awareness of these prohibitions and their commitment to comply strictly with them. Wherever possible, these prohibitions will also be included expressly and unequivocally in the contracts entered into with suppliers, advisers and business partners.

Where there is any doubt as to the purpose or nature of proposed expenditure, suppliers, advisers and business partners must inform CHUSE and obtain its authorisation before incurring it.

Covered Persons participating in the selection of suppliers, subcontractors or external collaborators must act impartially, transparently and objectively, applying quality and cost criteria to obtain the most advantageous offer. They must refrain from participating in any process in which their personal interests conflict with those of CHUSE.

ACCOUNTING RECORDS

CHUSE requires an appropriate accounting control system to be maintained and all transactions to be reported and recorded properly, accurately and in reasonable detail in the Company's books and accounting records. Those books and records must not contain false or misleading entries or statements. Accurate, appropriate and reasonably detailed documentation must be retained to support all transactions, and documents must be preserved in accordance with accounting legislation.

At a minimum, all financial transactions must:

- Be authorised in accordance with CHUSE's rules for approving expenditure.
- Be recorded in accordance with International Financial Reporting Standards, Generally Accepted Accounting Principles and the tax internal control standard approved by Management.
- Be reviewed periodically to identify and correct any accounting discrepancies, errors or omissions.

9.3. TRAINING AND COMMITMENT

CHUSE will provide members of the organisation with appropriate training on its ethical principles and on the duties and standards of conduct arising from its **Code of Conduct** and this **Anti-Corruption Policy**.

In particular, employees who are especially exposed to anti-corruption risks will receive annual training. They must also sign an annual **acknowledgement** accepting the **Policy** and the **Compliance Manual**, confirming that they have complied with the policies, practices and rules set out in this **Code, the Policies** and **the Manual** and that they are not aware of any breach.

9.4. DISCIPLINARY FRAMEWORK

Compliance with this **Policy** is mandatory. Any breach constitutes an infringement, and CHUSE will take the appropriate disciplinary action in accordance with employment legislation and the **Sanctions Framework**, without prejudice to any other liability that the offender may incur. CHUSE also reserves the right to take any measures it considers appropriate against business partners that fail to comply with the Policy.

Any employee or third party who knows or has reasonable grounds to suspect that this **Policy** has been breached must report it through the Ethics Channel. The Channel is both a means of reporting breaches of the rules in this **Policy** and a means of resolving questions about its application. CHUSE will take the necessary measures to prevent adverse consequences arising from reports made in good faith by members of its organisation in accordance with this Policy. The identity of anyone submitting a report through the Ethics Channel will be kept strictly confidential.

10. INFORMATION SECURITY, IT SYSTEMS AND DATA PROTECTION

CHUSE provides its employees with the IT resources it considers appropriate for the performance of their work. These resources must be used in a manner that respects the rights of other users, the integrity of the facilities and, where applicable, agreements and contracts with third parties. Each person providing services to CHUSE who is duly authorised to access its IT systems will be assigned specific computer equipment or a workstation and will have access only to the applications and personal data files needed to perform their duties.

To protect these resources, CHUSE has established appropriate security measures. Anyone with access to them is responsible for applying those measures and must know and comply with:

- [The Information Security Policy and Manual](#), which ensure the proper use of information systems.
- The [GDPR Handbook](#).
- The [Corporate Privacy Policy](#).
- The measures needed to maintain an appropriate level of security.

Compliance with these rules is mandatory for employees, without prejudice to any other obligations applicable to them.

The following is a brief summary of the principles developed in the [Corporate Privacy Policy](#), intended to mitigate the risk of criminal offences involving the unlawful acquisition and disclosure of secrets, unlawful access to information systems and damage to computer systems.

Each person's computer equipment or workstation will have a fixed operating system and application configuration, which may be changed only by the IT Department with Management's authorisation.

To avoid compromising the security measures in place, the following practices are prohibited unless authorised by CHUSE's Data Protection Officer and the IT Department:

- a) Any use for personal purposes.
- b) Installing software on computers or changing its configuration (operating system, programs, etc.).
- c) Connecting to networks or systems outside the CHUSE network.
- d) Removing equipment, confidential information or personal data, whether in electronic or non-electronic form, from the usual workplace without the corresponding authorisation and without first ensuring an appropriate level of security.

- e) Modifying or disabling security mechanisms that protect CHUSE's IT resources and information systems.

It is strictly prohibited to install or remove any software program, application or utility without Management's express written consent. Once authorised, installation or removal must be carried out by the IT Department. All installation or removal requests must be submitted through the [GLPI system](#).

Confidentiality of information:

Both during and after the employment relationship, CHUSE employees must maintain the strictest confidentiality regarding any information or data accessed during their employment with the Company that relate in any way to the Company's technology, accounts, customers, intellectual and industrial property rights, know-how, methods, organisation, personal data, contracts or activities, or those of any person or entity associated with them (hereinafter, '**Confidential Information**').

To ensure such confidentiality, users will have access only to the **Confidential Information** necessary to perform their duties, through the creation and assignment of user profiles and corresponding access passwords.

Each user is responsible for preventing unauthorised persons, INCLUDING OTHER COLLEAGUES, from using their assigned computer equipment to access information stored on that equipment or on the network where those persons are not authorised to do so. To this end, **whenever users leave their workstation (at the end of the working day, when going out, during breaks, rest periods, meetings, etc.), they must switch off or lock the equipment so that the session can be resumed only by re-entering their personal username and password.**

Confidential Information may be used by employees only during their professional relationship with the Company and strictly within the scope of their duties for the Company.

Immediately upon termination of the professional relationship with the Company for any reason, employees must return all documents, files and materials containing Confidential Information, including any IT devices in their possession, without retaining any copies or extracts. If the employment relationship is suspended, the Company also reserves the right to request the return of any files, documents, materials and IT devices held by the employee.

Failure by an employee to comply with this provision, whether during the employment relationship or after it has ended, will entitle the Company not only to impose any disciplinary sanctions applicable under current legislation, but also to claim compensation from the employee for any loss or damage caused by or arising from the breach of this duty of confidentiality.

For improved preservation, organisation, control and protection, all electronic documents relating to the Company must be stored on the server in the directory designated by the IT Department. They must not be stored on local hard drives or other devices unless expressly authorised by Company Management. The server is backed up to the cloud, allowing information to be recovered if it is deleted for any reason.

As a general rule, the use of USB drives or external hard drives is not authorised. The USB ports on CHUSE computers are therefore automatically disabled.

Employees are not permitted to install software. Installation must always be carried out by the IT Department to ensure compliance with the required security measures and the availability of appropriate support. Software may be installed and used only in accordance with the licences acquired.

Internet access must be used solely for professional purposes. Network connections must relate to the user's work and be made with a view to obtaining the greatest benefit from IT resources. Employees must be aware that they represent CHUSE when performing their duties and that their conduct must therefore reflect appropriate standards of ethics, professionalism, courtesy and responsibility.

For security and performance reasons, employees are informed that the IT Department may monitor Internet use in accordance with Article 20.3 of the Spanish Workers' Statute.

Email addresses using the CHUSE domain are Company property and are work tools that must be used solely for purposes relating to job duties. They are therefore professional tools, and authorised employees are responsible for how they are used. Any practice that could jeopardise the system's operation or proper use must be avoided.

All CHUSE employees and other Covered Persons must comply strictly with the data protection rules communicated through the [Onboarding Plan](#).

Employees' personal data must not be stored on computers provided by CHUSE or on any other computer.

11. UNLAWFUL ACQUISITION AND DISCLOSURE OF TRADE SECRETS

As established in the [Corporate Privacy Policy](#) and the Company's Internal Rules, everyone in the organisation, regardless of their position, must comply with the confidentiality undertaking and duty of secrecy in respect of Confidential Information and Trade Secrets accessed during their relationship with the Company.

Breaching the duty of secrecy may have employment, civil and criminal consequences.

All CHUSE employees and collaborators must ensure the confidentiality of all information processed by CHUSE. It is particularly important to note that the duty of secrecy continues after the employment relationship has ended.

To ensure compliance with this obligation, CHUSE, in its capacity as controller, requires every employee and collaborator to sign a **written confidentiality undertaking (Information and Duty of Secrecy Clause)** when their employment or collaboration with CHUSE begins.

Trade Secrets Act 1/2019 of 20 February is currently in force. It protects trade secrets and establishes a system of penalties where employees fail to respect them.

A trade secret **is defined as** any information or knowledge (technological, scientific, industrial, commercial, organisational or financial), regardless of the medium in which it is held, that:

- Is secret and therefore not generally known or readily accessible.
- Has actual business or commercial value because it is secret.
- Has been subject to reasonable measures to keep it secret.

Examples of trade secrets include lists of suppliers or customers, commercial strategies, business plans, information on the Company's internal operations, and financial, accounting or budgetary data.

Information constituting a Trade Secret may not be copied, supplied, disclosed or used by an employee outside the performance of their duties for the Company or for purposes other than those established or authorised by the Company.

A breach of trade secrecy includes obtaining a Trade Secret without its owner's consent (including unauthorised access to, appropriation or copying of documents, objects, materials, files or other media), breaching the confidentiality undertaking given by an employee to CHUSE, or any other conduct considered contrary to honest commercial practices.

The duty of secrecy is binding both while services are being provided and after the relationship with the Company has ended, irrespective of the reasons for or manner of its termination.

CHUSE employees must therefore respect at all times the confidentiality of information, including personal data accessed in the course of their employment with CHUSE, and comply with trade secrets legislation. Otherwise, CHUSE may take any legal measures it considers appropriate, including disciplinary action and claims for

compensation for loss or damage. Where remuneration has been received for the disclosure, use or dissemination of such information, CHUSE may also demand payment to the Company of that remuneration or its equivalent value.

12. ACCOUNTING AND TAX OBLIGATIONS. PROTECTION OF CHUSE'S ASSETS AND PREVENTION OF MONEY LAUNDERING

CHUSE will maintain complete, accurate and traceable accounting, tax and financial records prepared in accordance with applicable legislation and its internal procedures. The financial statements and other documentation must present a true and fair view of the organisation's economic and financial position and net assets. Concealing, altering or falsifying transactions, or maintaining unrecorded funds, assets, liabilities or transactions, is prohibited.

No employee or other Covered Person may authorise, carry out or assist with transactions intended to defraud the tax authorities, conceal tax-relevant information, fabricate expenses or transactions, use false or inaccurate invoices, or alter accounting or financial information. All tax obligations must be fulfilled correctly and within the statutory time limits.

Employees and other Covered Persons must use CHUSE's assets and resources responsibly and diligently, and solely for authorised professional purposes. This obligation covers tangible and financial assets as well as information, IT systems, intellectual and industrial property rights and other intangible assets. Any action that could cause their loss, deterioration, misuse, misappropriation, fraudulent use or impairment must be avoided.

Receipts and payments must be processed in accordance with the Rules on Receipts and Payments and on Cash and Banking, as well as the applicable internal procedures. As a general rule, cash receipts or payments are not permitted, except for expressly authorised small amounts processed in accordance with the [Purchasing](#) Procedure and the other controls in place. Every transaction must relate to genuine goods or services, be duly authorised and be supported by invoices, contracts, purchase orders, delivery notes or other sufficient documentary evidence. Issuing bearer cheques, making payments to accounts other than verified accounts or to third parties unrelated to the transaction, and artificially splitting payments to circumvent internal controls are expressly prohibited.

CHUSE will take reasonable measures to prevent its activities from being used for money laundering, terrorist financing or the transfer of funds of unlawful origin. Employees and other Covered Persons must pay particular attention to unusual transactions or those lacking economic justification; payments requested by persons or entities other than the contracting party; the unjustified use of cash; refusals to provide identification or contractual information; and any other red flag that may cast doubt on the identity, integrity or legitimacy of the parties, the

funds or the transaction.

Any irregularity or red flag must be reported immediately through the established internal channels. Until the transaction has been reviewed and authorised by the relevant functions, the person who detected the issue must refrain from carrying it out or assisting with it.

13. INTELLECTUAL AND INDUSTRIAL PROPERTY

CHUSE and Covered Persons must exercise particular care in protecting intellectual and industrial property rights and other intangible assets, whether belonging to CHUSE or to third parties. This protection covers, among other things, trade marks, trade names, domain names, patents, designs, projects, plans, software, source code, databases, manuals, photographs, videos, methodologies, processes, technologies, specialised technical knowledge, know-how and trade secrets.

Rights owned, licensed or lawfully used by CHUSE may be used only to perform authorised professional duties and in accordance with the established conditions, procedures and security measures. They must not be used for personal benefit or for the benefit of third parties, nor may they be reproduced, modified, assigned, disclosed, exploited or removed from CHUSE facilities or systems without proper authorisation.

Covered Persons must also respect third-party intellectual and industrial property rights. Software, content, images, publications, databases and other materials must not be installed, downloaded, copied, reproduced, distributed, transformed or used without the appropriate licence, authorisation or legal entitlement. This obligation also applies to open-source software, which must be used in accordance with its specific licence terms.

Protected content or information may be incorporated into digital platforms, cloud services, artificial intelligence tools or other external systems only where those systems have been approved in advance by CHUSE and their use is compatible with the relevant rights, confidentiality obligations and information security policies.

Creations, developments, documents, materials and results produced in the performance of professional duties will be subject to the ownership and use arrangements established by applicable legislation, contracts and internal rules. Covered Persons must assist in protecting CHUSE's rights and refrain from any action that could compromise their registration, preservation, exploitation or defence.

When their professional relationship ends, or whenever requested, Covered Persons must return all documents, media and materials containing CHUSE intangible assets or protected information, without retaining copies or continuing to use them. The duties of confidentiality and protection of trade secrets continue after the relationship

ends.

Any unauthorised use, suspected infringement or loss of protected information must be reported immediately through the established internal channels so that the necessary measures can be taken to protect the rights and interests of CHUSE and third parties.

14. HUMAN RIGHTS POLICY

Human rights are inherent to every person, without distinction on grounds of nationality, place of residence, sex, national, social or ethnic origin, colour, religion, language, age, disability, sexual orientation, gender identity or expression, political or trade union opinion, economic circumstances or any other personal or social status.

CHUSE is committed to respecting, protecting and promoting human rights in all its activities, operations and business relationships, in accordance with applicable legislation and the principal national and international standards in this area.

The principles and commitments set out in this section must be interpreted in accordance with [CHUSE's Human Rights Policy](#) and its other internal policies and rules, particularly the [Integrated Policy, the Criminal Compliance Policy and Manual, the Policy Guaranteeing the Rights of LGTBQ+ People, the Equality Plan](#), the [protocols for preventing and responding to harassment and violence](#), and the internal rules on [data protection and information security](#).

CHUSE's commitments are aligned with, among others, the following:

- The International Bill of Human Rights.
- The United Nations Guiding Principles on Business and Human Rights.
- The International Labour Organization Declaration on Fundamental Principles and Rights at Work and the ILO Fundamental Conventions.
- The United Nations Convention on the Rights of Persons with Disabilities.
- The European Convention on Human Rights.
- The revised European Social Charter.
- The Charter of Fundamental Rights of the European Union.
- The European Pillar of Social Rights.

- The United Nations Sustainable Development Goals.
- European legislation on sustainability, corporate due diligence and the prohibition of products made using forced labour.
- Applicable Spanish legislation on employment, equality, non-discrimination, harassment prevention, whistleblower protection and other areas related to human rights.

14.1. SCOPE AND APPLICATION

The principles of this Policy apply directly to all CHUSE management activities and will guide the Company's approach to human rights in its relationships with employees, customers, suppliers and the community in which it operates.

The purpose of this Policy is to minimise the risk of human rights violations by establishing principles and guidelines for human rights due diligence that make it possible to identify, prevent, mitigate and remedy potential adverse impacts. CHUSE's actions therefore include:

- a) Establishing commitments.
- b) Assigning responsibilities.
- c) Correcting errors and poor practices.
- d) Providing training on these matters.

CHUSE Management will use every means at its disposal to ensure compliance with the commitments in this Policy and to ensure that the Policy is made public and communicated internally and externally.

14.2. COMMITMENTS TO HUMAN RIGHTS

14.2.1. COMMITMENTS TO CHUSE EMPLOYEES

CHUSE's relationships with its employees, and relationships among employees, will be based on compliance with the following commitments:

(a) Eradication of child labour

CHUSE rejects all forms of child labour and will ensure compliance with applicable legislation and international conventions on the minimum age for employment and the protection of children and young people.

(b) Prohibition of forced labour, slavery and trafficking in persons

CHUSE will not tolerate any form of forced or coerced labour, slavery, servitude, human trafficking or practices associated with modern slavery, both in its own activities and in its supply chain.

(c) Decent work and fair working conditions

CHUSE will guarantee decent working conditions and remuneration appropriate to the duties performed and the time worked. Remuneration must not be lower than that established by applicable legislation and collective agreements and must be paid regularly, promptly and directly.

Applicable rules on working hours, rest periods, holidays, overtime and Social Security will be respected. Contractual terms, working hours and remuneration must be communicated clearly, accessibly and comprehensibly.

(d) Equal opportunities and remuneration

Recruitment, hiring, promotion, training and professional development will be based on objective criteria of merit, ability, competence and suitability.

CHUSE will guarantee equal opportunities and equal pay for work of equal value, preventing all direct and indirect discrimination.

(e) Diversity, inclusion and non-discrimination

CHUSE will promote an inclusive workplace that respects diversity and is free from discrimination.

No discriminatory treatment will be tolerated on grounds of race, nationality, social or ethnic origin, age, sex, marital status, sexual orientation, gender identity or expression, ideology, political or trade union opinion, religion, belief, disability or any other personal or social condition or circumstance.

(f) Prevention of harassment and violent behaviour

CHUSE maintains zero tolerance of workplace harassment, sexual harassment, sex-based harassment, harassment based on sexual orientation, gender identity or gender expression, and any threat, intimidation, violence or abusive, hostile, humiliating or offensive conduct.

These situations will be managed in accordance with internal protocols and applicable regulations.

(g) Responsible recruitment and protection of migrant workers

When migrant workers are recruited, CHUSE will ensure that:

- They are not charged recruitment fees or costs.
- No fraud, deception, coercion or omission of relevant information occurs.
- They fully understand their contract and its terms.
- They retain their identity documents, permits and visas.
- Their personal documents are not retained beyond what is strictly necessary and legally permitted.
- They may freely terminate their employment in accordance with the applicable legal and contractual procedure, without undue penalties.

(h) Occupational health and safety

CHUSE will provide a safe and healthy working environment, the necessary protective equipment and appropriate training and information to prevent accidents and ill health.

Preventive measures will be updated periodically and integrated at every level of the organisation. Employees must comply with health and safety rules, use the means provided to them correctly and look after their own safety and that of others.

(i) Freedom of association, assembly and collective bargaining

CHUSE will respect and protect employees' rights to freedom of association, assembly, representation, organisation, collective bargaining and strike action, without interference, retaliation or discrimination arising from the legitimate exercise of those rights.

(j) Work-life balance, rest and the right to disconnect

CHUSE will respect the rights to holidays, rest, work-life balance and disconnection from work, promoting measures aimed at employees' physical and emotional well-being.

(k) Training and professional development

CHUSE will promote training and development initiatives that enable employees to perform their duties safely, develop their skills and adapt to organisational and professional needs.

(l) Human rights awareness

CHUSE will communicate its human rights commitments and promote training on ethics, integrity and human rights so that employees understand their rights and obligations and the mechanisms available for reporting potential breaches.

(m) Privacy and data protection

CHUSE will respect the rights to privacy, honour and protection of personal data of everyone with whom it interacts.

Personal, confidential, restricted or privileged information will be processed in accordance with legislation and internal information security rules. CHUSE will implement the organisational, technical and cybersecurity measures needed to protect information for which it is responsible.

14.2.2. COMMITMENTS TO CUSTOMERS AND SUPPLIERS

CHUSE requires its employees to respect people, their dignity and their fundamental values, as established in this **Code of Conduct**. The Company also undertakes to conduct its activities to a high professional standard, enabling its employees to provide efficient services tailored to the needs of customers and users, with a focus on service excellence and quality. CHUSE is also committed to maintaining relationships with them based on transparency, confidentiality and non-discrimination.

CHUSE also undertakes to act impartially and objectively when selecting subcontractors, suppliers and external collaborators, applying value-for-money criteria and avoiding conflicts between personal interests and those of the Company.

It will also ensure that subcontractors, suppliers and external collaborators are informed of CHUSE's human rights commitments, that they endorse those commitments, and that mechanisms are established to detect poor practices in this area.

For the purposes of complying with this Policy, CHUSE also has a [complaints handling procedure](#) that describes the steps to be followed when assisting users.

14.2.3. COMMITMENTS TO THE COMMUNITY AND LOCAL ENVIRONMENT

CHUSE is committed to ensuring the greatest possible respect for human rights in the local environment and the communities in which it operates. To this end, CHUSE undertakes to conduct its activities in accordance with:

- Fair competition, avoiding any conduct or procedure that undermines it.
- Compliance with current labour and tax regulations.

- Respect for the environment when conducting activities, minimising any adverse effects they may cause.

14.3. IMPLEMENTATION, COMPLIANCE AND COMMUNICATION OF THE HUMAN RIGHTS POLICY

A human rights culture is embedded in the Company through training to ensure that all CHUSE employees properly understand this **Policy**. In implementing the Policy, due account will be taken of this **Code**, as approved by the Compliance Committee.

CHUSE will also periodically analyse human rights matters relating to its activities and implement due diligence processes to assess the risk of non-compliance, on the basis of which it will propose measures to prevent or remedy adverse impacts.

It will also maintain and publicise effective reporting and complaint mechanisms so that people directly affected by its operations can bring any potential human rights impact to CHUSE's attention.

CHUSE employees must report any suspected breach of the commitments set out in this Policy of which they become aware, as well as any breach of the other guidelines and standards of conduct established in this **Code**. Reports may be made anonymously.

For this purpose, CHUSE has an Ethics Channel for receiving reports of irregular conduct or activities, through which employees may submit any queries about these and other matters in complete confidence.

CHUSE expects all employees to show a high level of commitment to complying with this Policy. Any breach may result in the corresponding disciplinary measures.

14.4. OVERSIGHT AND MONITORING SYSTEMS

CHUSE's Criminal and Regulatory Compliance Committee is responsible for overseeing compliance with the Human Rights Policy. The Policy is monitored and evaluated through the Committee and the Ethics Channel, which can be used to report irregular conduct or any breach of the rules in this Code by emailing canaletico@chsonespases.com or submitting a written report in a sealed envelope addressed to the Criminal and Regulatory Compliance Body.

The Committee will be responsible for carrying out due diligence processes in the course of its work, analysing the indicators and information needed to understand and assess human rights risks and adopting the measures necessary to prevent and mitigate them.

Mechanisms and procedures are therefore established to minimise the risk of poor human rights practices, including:

- Developing employee training initiatives on ethics, integrity and human rights.
- Promoting and encouraging suppliers, subcontractors and collaborating companies to formalise their commitment to human rights and, if they do not have their own policy, to endorse CHUSE's Policy.

The Human Rights Policy will be reviewed periodically to ensure its continued suitability and effective implementation. All revisions will be subject to approval by CHUSE's Criminal and Regulatory Compliance Body.

15. RIGHT TO DISCONNECT POLICY

Technological devices and tools facilitate professional activities, but they may also lead to an undue extension of working hours, inadequate boundaries between working time and rest time, and risks related to hyperconnectivity, technostress and digital fatigue.

CHUSE recognises and guarantees employees' right to disconnect outside their working hours, in order to respect their rest periods, leave and holidays, protect their personal and family privacy, support work-life balance, and prevent risks to their health and safety.

The right to disconnect will be exercised in accordance with Article 88 of Organic Law 3/2018 on Personal Data Protection and the Guarantee of Digital Rights; Article 20 bis of the Spanish Workers' Statute; Article 18 of Law 10/2021 on remote working; the applicable collective bargaining rules; and CHUSE's Right to Disconnect Policy and Protocol.

For these purposes, the right to disconnect means employees' right not to access, deal with or respond to work-related communications, calls, emails, messages or requests made through technological tools outside their working hours, except in the exceptional circumstances set out in this section.

Exercising this right will help to:

- Respect rest periods, leave and holidays.
- Promote work-life balance.
- Avoid unnecessary extensions of the working day and situations of digital presenteeism.
- Protect personal and family privacy.
- Prevent risks arising from hyperconnectivity, such as technostress, digital fatigue and occupational burnout.
- Promote a reasonable, efficient and healthy use of information and communication technologies.

- Promote an organisational culture based on planning, efficiency and a focus on results.

15.1. SCOPE OF APPLICATION

The right to disconnect is recognised for all CHUSE employees, including those in management, supervisory or other positions of responsibility, regardless of:

- Their type of contract.
- Their working hours or working-time arrangements.
- Their job or seniority level.
- Whether their work is on-site, remote or hybrid.
- The technological devices or channels they use.

The right applies outside working hours and during daily and weekly rest periods, leave, holidays, suspensions of the employment contract and any other periods of absence recognised by law or collective agreement.

Outside working hours, employees are not required to:

- Check their corporate email account.
- Answer work-related calls.
- Read or reply to messages sent via WhatsApp, instant messaging apps, or other channels.
- Connect to corporate applications, platforms, or systems.
- Carry out work-related tasks using personal or corporate devices.

Failure to respond to a communication received outside working hours will not be considered a breach, neglect or lack of diligence unless one of the exceptional circumstances set out in section 15.4 applies.

Management and middle managers have a particular responsibility to promote and respect this right and must avoid conduct that creates or could create an expectation of permanent availability within their teams.

15.2. PRINCIPLES GOVERNING THE RIGHT TO DISCONNECT

1.1. The right to disconnect is recognised for all employees of the Concessionaire.

1.2. An employee's right to 'disconnect from technology' means the right to have no contact with work-related digital tools during rest periods, outside their daily working hours and/or during weekly and/or annual rest periods.

Rules are therefore established for the proper use of digital tools, together with preventive mechanisms to avoid excessive connectivity and protect employees who wish to exercise this right.

1.3. The right to disconnect does not prohibit employees from using digital tools outside working hours, as disconnection is a right, not an obligation. Employees may decide whether or not to connect outside their usual working hours. In all cases, however, they must ensure that minimum daily, weekly and annual rest periods are respected.

1.4. An employee may be contacted outside working hours in an urgent or serious situation. Such exceptional situations range from major risks or environmental incidents (flooding, structural collapse, etc.) to computer virus incidents, accidents, health risks and other matters within the hospital care environment that require urgent intervention.

1.5. All Concessionaire employees who are at risk of excessively extended working hours and, consequently, increased workload or failure to disconnect from work during rest periods must receive awareness-raising and training on the efficient and responsible use of digital tools.

1.6. In applying the right to disconnect, account must be taken of the Concessionaire's responsibility to ensure service delivery and meet customer needs. The employee's role and seniority also affect how this right applies.

15.3. ACTIONS AND MEASURES TO GUARANTEE EMPLOYEES' RIGHT TO DISCONNECT

CHUSE will implement the following measures:

Sending communications during working hours

Emails, messages, calls and other work-related communications should preferably be sent or made during the recipient's usual working hours.

Before sending a communication outside those hours, consideration must be given to whether it is necessary or can wait until the next working day.

Anyone sending a communication outside the recipient's working hours must accept that the recipient may not read or respond to it until they return to work.

Use of scheduled or delayed sending

Anyone who drafts an email or message outside their working hours should preferably use:

- The draft function.
- The scheduled or delayed send function.

- Other features that allow the communication to be delivered during the recipient's working hours.

This measure applies particularly to communications sent by Management, department heads, service managers and middle managers.

Out-of-office replies during absences

An employee who will be absent for more than one day must activate an automatic out-of-office reply whenever this is necessary given the nature of their position.

The message should state:

- The approximate period of absence.
- That the email account will not be monitored during that period.
- The alternative contact person or unit.
- The details necessary to contact that person or unit.

The alternative contact will be determined by the area of activity, the duties performed and the expected duration of the absence.

Appropriate use of communication channels

Communications must be made through the established corporate channels.

Personal telephone numbers and private messaging applications may be used for work-related communications only where authorised or necessary due to the nature of the activity.

Professional messaging groups should not be used outside working hours for routine communications that can wait until the next working day.

Email best practices

The following practices will be promoted to avoid technological overload and hyperconnectivity:

- Reduce unnecessary emails.
- Use direct communication where it is more efficient.
- Avoid copying in people who are not directly involved in the matter.
- Use clear subject lines that identify the purpose and priority of the communication.
- Do not use terms such as 'urgent' or 'immediate' unless there is a genuine need that justifies them.
- Avoid unnecessarily long message chains.
- Do not request read receipts or an immediate response unless essential.
- Schedule delivery when a message is drafted outside the recipient's working hours.

Organising meetings and activities

As a general rule, meetings, meeting invitations, training activities and other professional activities must be scheduled within the working hours of those invited.

They must be scheduled so as not to extend working hours unnecessarily or interfere with rest periods, leave or work-life balance.

Training and awareness-raising

CHUSE will provide periodic training and information for employees, Management and middle managers on:

- The contents of the Right to Disconnect Policy and Protocol.
- The efficient use of technological tools.
- The risks associated with technological dependence and hyperconnectivity.
- Preventing technostress, digital fatigue and occupational burnout.
- The responsibilities of those who coordinate or lead teams.

Preventing psychosocial risks

The right to disconnect will be taken into account in psychosocial risk assessments.

Where excessive connectivity, regular extensions of working hours, repeated communications outside working hours or an expectation of permanent availability are detected, CHUSE will analyse the causes and adopt the necessary organisational or preventive measures.

Conduct of Management and middle managers

Management, department heads and middle managers must act as role models in respecting the right to disconnect. In particular, they must:

- Properly plan tasks and communications.
- Avoid routine requests outside working hours.
- Not demand immediate responses during rest periods.
- Not treat a failure to respond outside working hours negatively.
- Make it clear when a communication does not require immediate attention.
- Use delayed sending when drafting communications outside their teams' working hours.

15.4. EXCEPTIONS

As a general rule, the right to disconnect must be respected. However, an employee may be contacted outside working hours where an extraordinary situation:

- Is urgent, serious or unforeseeable.
- Requires action that cannot be reasonably delayed.
- Relates to the continuity, safety or proper delivery of CHUSE's services.
- Cannot be resolved through ordinary organisational, cover or on-call arrangements.

Exceptional situations may include:

- Accidents or serious risks to people.
- Health emergencies.
- Serious information security or cybersecurity incidents.
- Failures or critical incidents affecting essential facilities or services.
- Serious environmental incidents, such as floods, landslides or spills.
- Situations that could immediately compromise the continuity or safety of hospital operations.
- Urgent requests from competent authorities or bodies that cannot be dealt with during ordinary working hours.

These communications must be:

- Exceptional and infrequent.
- Necessary and proportionate.
- Duly justified.
- Limited to the time strictly necessary.
- Directed only to those whose involvement is necessary.

Anyone performing Senior Management or Head of Service duties must keep their corporate telephone operational solely to deal with urgent or emergency situations requiring their intervention outside working hours.

This obligation does not imply general availability and does not justify routine communications outside working hours. On-call duties, availability periods or interventions outside normal working hours will be managed in accordance with the applicable legislation, collective agreement and employment conditions.

16. CRIMINAL COMPLIANCE POLICY AND MANAGEMENT SYSTEM

CHUSE has established a Criminal Compliance Management System to identify risks and/or conduct that could constitute an offence under the corporate criminal liability regime established by the Spanish Criminal Code. The system has been adapted, implemented and established to provide working methods aligned with Spanish criminal legislation for the prevention and detection of criminal offences.

A Criminal and Regulatory Compliance Committee **has been established** as the Criminal and Regulatory Compliance Body (OCPN). It has autonomous powers of initiative and control and is entrusted with overseeing the operation of and compliance with the management system.

This **Compliance Policy** expresses the organisation's commitment to achieving its criminal compliance objectives and meeting the expectations and needs of its stakeholders. CHUSE therefore undertakes to integrate criminal compliance principles into its management and processes, supported by audits and certifications in the field of criminal compliance.

The fundamental principles for achieving these objectives are:

- Commitment to meeting the requirements of the Hospital and/or those established by IB-Salut.
- Ensure compliance at all times with the rules and legislation applicable to the Criminal Compliance Management System.
- Identify the activities within which the offences to be prevented could be committed.
- **Prohibit the commission of criminal offences.**
- Minimise the organisation's exposure to criminal risks.
- Ensure that objectives are achieved through accountability and the involvement of the entire organisation, supported by staff commitment and the effective management of available resources.
- Commitment by the organisation to comply with the requirements established in this Policy and in the Criminal Compliance Management System.
- Require the reporting of suspicious facts or conduct relating to criminal risks, while guaranteeing confidentiality, protection against detrimental treatment (including retaliation) and the possibility of reporting anonymously.

- Ensure the authority of the Criminal and Regulatory Compliance Body (OCPN) through a collegiate body comprising several members, independent of the governing body, and give the OCPN autonomous powers of initiative and control, together with responsibility for developing and overseeing the operation of and compliance with the Criminal Compliance Management System.
- Maintain continual improvement.
- Ongoing training is a fundamental pillar of the organisation's approach to employee development, providing high-quality theoretical and practical training.
- Establish the Ethics Channel as the Internal Information System through which persons associated with CHUSE may report any irregularity, matter or concern relating to the risk of conduct that could constitute an unlawful or criminal act, without prejudice to the option of reporting directly to the Independent Whistleblower Protection Authority or any other competent authority, including the Public Prosecutor's Office.
- Establish the following as the general principles of the Internal Information System:
 - Ensure that reporting persons can fulfil their duty to report freely and without any fear of retaliation, provided that they have acted in good faith. Any sanction, disciplinary measure or retaliation merely for having submitted a report is strictly prohibited.
 - Prohibit any CHUSE person or body from retaliating, or allowing any other person to retaliate or attempt to retaliate, directly or indirectly, against persons who report in good faith. This prohibition includes threats and attempted retaliation.
 - Guarantee respect for the rights of the person concerned by the report, particularly their right to honour and the presumption of innocence.
 - Ensure that reports are submitted directly to the OCPN, without reporting persons having to notify their line manager or any other intermediate body beforehand.
 - Reporting persons are not required to identify themselves, as anonymous reports are permitted.
 - Ensure strict respect for the rights of both the person concerned by the report and the reporting person, including the rights established by applicable data protection legislation.

Failure to comply with the requirements of this Policy or those arising from the Criminal Compliance Management System will result in the disciplinary measures established in the [Disciplinary Framework](#), as well as any other legal action that the OCPN and the governing body consider appropriate.

This Compliance Policy is understood, implemented and kept up to date at every level of the organisation. It has the full commitment and support of the OCPN and Management and is established, developed and applied through the implemented Compliance Management System.

17. EQUALITY POLICY

The principle of equality is recognised both internationally and under Spanish law. Article 14 of the Spanish Constitution proclaims the right to equality and non-discrimination on grounds of sex. Article 9.2 establishes the obligation of public authorities to promote the conditions required for equality of individuals and the groups of which they form part to be real and effective.

Organic Law 3/2007 of 22 March on the Effective Equality of Women and Men (hereinafter, the '**LOI**') and Royal Decree-Law 6/2019 of 1 March on urgent measures to guarantee equal treatment and opportunities for women and men in employment and occupation aim to give effect to the right to equal treatment and opportunities for women and men, particularly by eliminating sex-based discrimination in every area of life.

In the field of employment, the **LOI** requires companies to respect the principle of equality and to adopt measures aimed at preventing any form of discrimination between women and men. Specifically, it provides for the preparation and implementation of an **Equality Plan** as a structured set of measures adopted following an assessment of the situation, including the necessary objectives, strategies and practices and a system for monitoring and evaluating their implementation.

Concesionaria Hospital Universitario Son Espases, S.A. (hereinafter, the '**Company**' or '**CHUSE**') is governed by generally applicable legislation, including Royal Legislative Decree 2/2015 of 23 October approving the consolidated text of the Spanish Workers' Statute (hereinafter, the '**ET**').

CHUSE fully recognises the importance of the principle of equality and is committed to implementing measures aimed at improving equal opportunities in the workplace. The Company is also committed to work-life balance and excellence, as it believes that the highest level of professional excellence can be maintained while enabling employees to achieve an appropriate balance between their professional, personal and family lives.

CHUSE is committed to creating a diverse environment and is proud to be an equal opportunities employer. All candidates are considered for selection regardless of race, colour, religion, gender, gender identity or expression, sexual orientation, national origin, genetic information, age or veteran status. The Company is also committed to fair employment practices relating to citizenship and immigration status.

Achieving substantive equality requires a gender perspective to be integrated throughout the organisation's management, policies, levels and areas, including access to the Company, recruitment and working conditions, promotion, training, remuneration, work-life balance and occupational health.

The Equality Plan uses different terms defined in accordance with the **LOI**:

- 1. The principle of equal treatment between women and men** (Article 3 LOI) - This means the absence of any direct or indirect discrimination on grounds of sex, especially discrimination arising from maternity, family responsibilities or marital status.
- 2. Direct discrimination on grounds of sex** (Article 6 LOI) - A situation in which a person is, has been or could be treated less favourably than another in a comparable situation on account of their sex.
- 3. Indirect discrimination on grounds of sex** (Article 6 LOI) - A situation in which an apparently neutral provision, criterion or practice places persons of one sex at a particular disadvantage compared with persons of the other sex, unless that provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are necessary and appropriate.
- 4. Sexual harassment** (Article 7 LOI) - Any verbal or physical conduct of a sexual nature that has the purpose or effect of violating a person's dignity, particularly where it creates an intimidating, degrading or offensive environment.
- 5. Sex-based harassment** (Article 7 LOI) - Any conduct relating to a person's sex that has the purpose or effect of violating their dignity and creating an intimidating, degrading or offensive environment.
- 6. Discrimination on grounds of pregnancy or maternity** (Article 8 LOI) - Any unfavourable treatment of women relating to pregnancy or maternity constitutes direct discrimination on grounds of sex.
- 7. Positive action** (Article 11 LOI) - Specific measures in favour of women intended to correct clear situations of de facto inequality compared with men. Such measures, which will apply for as long as those situations persist, must be reasonable and proportionate to the objective pursued in each case.
- 8. Equal treatment and opportunities for women and men** (Article 3 LOI) - This means the absence of any direct or indirect discrimination on grounds of sex, especially discrimination arising from maternity, family responsibilities or marital status.

18. PROTOCOL FOR DEALING WITH WORKPLACE HARASSMENT, SEXUAL HARASSMENT, SEX-BASED HARASSMENT, AND HARASSMENT BASED ON SEXUAL ORIENTATION, GENDER IDENTITY OR GENDER EXPRESSION

Physical and/or psychological violence and harassment, specifically sexual harassment and sex-based harassment, may constitute offences under the Spanish Criminal Code. This internal procedure therefore operates independently of any legal action that may be brought before an administrative or judicial authority.

Everyone has the right to be treated with dignity, to have their moral integrity respected and to be free from discrimination. To ensure that the workplace protects these rights, Concesionaria Hospital Universitari Son Espases (hereinafter, 'CHUSE') is committed to creating a working environment in which the dignity and sexual freedom of every employee are respected.

Through this Protocol, CHUSE declares zero tolerance throughout its organisation of discriminatory conduct and conduct constituting workplace harassment, sexual harassment, sex-based harassment, or harassment based on sexual orientation, gender identity and/or gender expression. The Policy Guaranteeing the Rights of LGTBQ+ People also guarantees and promotes the right of lesbian, gay, trans, bisexual and intersex people to substantive equality and freedom from discrimination, harassment and/or discriminatory violence.

CHUSE declares that harassment and discrimination violate human dignity and will therefore neither permit nor tolerate harassment in the workplace. Through this Protocol, CHUSE expresses zero tolerance of physical, verbal or psychological violence in the workplace and states that discriminatory conduct, degrading treatment, harassment or violence against any person will not be accepted under any circumstances.

CHUSE establishes as a fundamental principle that everyone is entitled to proper, respectful and dignified treatment and to respect for their privacy and physical and moral integrity. No person may under any circumstances be subjected to degrading, humiliating or offensive treatment on grounds of birth, race, sex, age, sexual orientation or identity, gender expression, religion, opinion or any other personal or social condition or circumstance, including employment status.

By adopting this Protocol, CHUSE emphasises its commitment to preventing and responding to workplace harassment, sexual harassment, sex-based harassment and harassment based on sexual orientation, gender identity or gender expression in any form. The Protocol applies to everyone providing services within the organisation, whether employed directly or supplied by another company, and to persons who provide services or collaborate with the organisation without an employment relationship, including trainees, interns and volunteers.

CHUSE also undertakes to inform both companies to which it assigns its own staff and companies whose staff work at CHUSE of the existence of this Protocol and the need for strict compliance. The obligation to comply with the Protocol will therefore be included in contracts entered into with other companies.

This Protocol complies with Articles 46.2 and 48 of Organic Law 3/2007 of 22 March on the Effective Equality of Women and Men; Royal Decree 901/2020 of 13 October regulating equality plans and their registration and amending Royal Decree 713/2010 of 28 May on the registration and filing of collective labour agreements; Article 14 of Law 31/1995 of 8 November on Occupational Risk Prevention; Law 15/2022 of 12 July on Comprehensive Equal Treatment and Non-Discrimination; Organic Law 10/2022 of 6 September on the Comprehensive Guarantee of Sexual Freedom; and Law 4/2023 of 27 February on the Substantive and Effective Equality of Trans People and Guaranteeing the Rights of LGBTI People.

By committing to the measures set out in this Protocol, CHUSE expressly demonstrates and communicates its intention to adopt a proactive approach both to preventing harassment, through awareness-raising and information on conduct not tolerated by the Company, and to disseminating good practices and implementing all measures needed to handle reports and complaints and resolve each case as appropriate.

Everyone is also guaranteed the right to initiate the procedures established in this Protocol and elsewhere in the system without fear of intimidation or unfair, discriminatory or unfavourable treatment. This protection applies equally to anyone who submits a report, provides information relating to a report or otherwise assists at any stage of the procedure described in this Protocol.

CHUSE is committed to achieving safe and respectful workplaces for everyone. Combating all forms of discrimination is a priority and an active commitment. For further information, consult the [Protocol for Dealing with Workplace Harassment, Sexual Harassment, Sex-Based Harassment, and Harassment Based on Sexual Orientation, Gender Identity or Gender Expression](#).

19. COMPREHENSIVE GUARANTEE OF SEXUAL FREEDOM POLICY

Organic Law 10/2022 of 6 September on the Comprehensive Guarantee of Sexual Freedom includes significant employment-related provisions intended to prevent sexual violence at work and recognise a specific employment status for female employees who are victims of sexual violence, equivalent to that of victims of gender-based violence. The main measures taken in relation to this Law are:

- Promoting working conditions that prevent criminal offences and other conduct against sexual freedom and moral integrity at work.

- Establishing specific procedures to prevent such conduct and handle reports and complaints.
- Providing all employees with training and awareness-raising on comprehensive protection against sexual violence.
- Including sexual violence among the occupational risks considered in risk assessments for the different positions held by female employees.
- Integrating a gender perspective into the organisation so that workplaces are accessible and safe for all female employees.

CHUSE has specific procedures to prevent criminal offences and other conduct against sexual freedom and moral integrity at work, with a particular focus on sexual harassment and sex-based harassment.

It also handles reports or complaints made by victims of such conduct, including conduct in the digital environment, through the **Ethics Channel** (see section 6 of this document).

20. POLICY GUARANTEEING THE RIGHTS OF LGTBIQ+ PEOPLE

CHUSE recognises everyone's right to equal treatment and opportunities and to freedom from discrimination, harassment or violence on grounds of sexual orientation, sexual or gender identity, gender expression, sex characteristics or family diversity.

The Policy Guaranteeing the Rights of LGTBIQ+ People seeks to guarantee and promote the substantive and effective equality of lesbian, gay, trans, bisexual and intersex people and others representing sexual, family and gender diversity, and to prevent, remedy and eliminate all forms of discrimination, stereotyping and prejudice.

This Policy applies to all CHUSE staff, regardless of their type of contract or position, and to temporary agency workers while they provide services. Its principles must also be respected in relationships with collaborators, suppliers, patients, customers and users.

CHUSE undertakes to:

- Guarantee equal treatment and opportunities in access to employment, recruitment, training, job grading, career progression, working conditions, leave and employee benefits.
- Apply objective, bias-free criteria in recruitment and promotion processes and use respectful and inclusive language.

- Promote diverse, safe and inclusive workplaces by applying zero tolerance to all discriminatory conduct, harassment, violence and LGTBI-phobia.
- Provide training and awareness-raising for all staff, particularly Management, middle managers and those responsible for recruitment or personnel management.
- Guarantee the confidentiality and protection of personal data relating to sexual orientation, gender identity or expression and sex characteristics.
- Prohibit retaliation against anyone who reports possible discriminatory conduct in good faith or cooperates in an investigation.
- Include respect for the rights of LGTBIQ+ people among the criteria for selecting and establishing relationships with new suppliers.

CHUSE will provide practical support and protection to trans people who request it during their transition. Their chosen name and gender identity will be respected in communications and internal systems, except where there is a legal obligation to use civil registry details, in which case disclosure will be minimised and access to the information restricted. Temporary adjustments to working hours may also be made for medical reasons, and the use of uniforms, toilets, changing rooms and other facilities will be guaranteed in accordance with the person's identity.

Anyone who becomes aware of possible discrimination, harassment or violence against an LGTBIQ+ person must report it through the Ethics Channel or the mechanisms established in the Reporting Breaches and Irregularities Procedure and the Anti-Harassment Protocol.

Reported conduct will be investigated confidentially and impartially, with full respect for the rights of those involved. Where a breach is substantiated, CHUSE will take the appropriate preventive, corrective or disciplinary measures in accordance with the disciplinary framework, the applicable collective agreement and current legislation.

For further information, consult the [Policy Guaranteeing the Rights of LGTBIQ+ People](#).

21. INFORMATION SECURITY AND DATA PROTECTION POLICY

CHUSE considers information security essential to the provision of its services and is committed to protecting information, personal data, systems and technological resources against loss, improper access, cyberattacks, alteration, disclosure or unauthorised use.

To this end, CHUSE has an Information Security Management System based on identifying, protecting, detecting, responding to and recovering from risks and incidents that may affect its activities. The system will be reviewed and improved periodically in line with changes in risks, technologies, organisational needs and applicable legislation.

CHUSE's actions in the field of information security are based on the following principles:

- **Confidentiality:** information may be accessed and used only by duly authorised persons.
- **Integrity:** information must be kept complete and accurate and protected against unauthorised alteration or manipulation.
- **Availability:** information and systems must be accessible to authorised persons when needed.
- **Resilience:** CHUSE will adopt the technical and organisational measures needed to prevent, withstand, respond to and recover from incidents.
- **Lawfulness:** information will be processed in accordance with applicable legislation, contractual requirements and Internal Rules.

CHUSE undertakes to:

- Assess and treat information security risks.
- Implement controls to prevent, detect, manage and remedy incidents.
- Protect personal data, privacy, intellectual property, and confidential information.
- Ensure continuity of critical processes and services.
- Clearly assign responsibilities for security.
- Train employees and raise their awareness of the secure use of information and technological resources.
- Record, analyse and manage security incidents.
- Control changes that may affect information security.
- Require suppliers, subcontractors and other third parties to comply with the security measures applicable to them.
- Periodically review the effectiveness of the controls implemented and adopt the necessary measures to correct the deviations detected.

All employees, collaborators and other persons authorised to access CHUSE information or systems must:

- Know and comply with the [Information Security Policy](#), data protection regulations and applicable internal instructions.
- Use only authorised equipment, applications, networks, and services.
- Protect their access credentials and not share them with anyone else.
- Access only the information needed to perform their duties.
- Maintain the confidentiality of information both during and after their relationship with CHUSE.
- Avoid any action that may compromise the security of systems or information.
- Immediately report any loss of information, improper access, suspicious email, infection, error, vulnerability or incident of which they become aware.
- Cooperate in implementing the security, continuity and recovery measures established by CHUSE.

The IT resources and information systems provided by CHUSE are work tools and must be used responsibly, securely and for their intended professional purpose. Without the corresponding authorisation, no one may install software, change configurations, connect external devices or services, disable security measures or remove information from authorised environments.

Failure to comply with the Information Security Policy or the rules in this section may result in corrective or disciplinary measures, without prejudice to any applicable legal liability.

For further information, consult [the Information Security Policy](#), [the Corporate Privacy Policy](#), [the Data Protection Manual](#), the Internal Rules of the Information Security Management System, and the incident reporting and management procedures.

22. EXAMPLES OF BREACHES OF THE CODE OF CONDUCT

By way of illustration, the following are examples of breaches of the Code:

- Breaching legal provisions in a manner that results in penalties imposed by the authorities, financial loss or future liabilities for the Company.
- Negligently disregarding policies, rules or practices for the proper management of the Company, causing it serious harm.
- Engaging in any form of harassment.

- Showing signs of drug or alcohol intoxication and/or engaging in immoral conduct on Company premises.
- Discriminating against, intimidating or harassing another person on grounds of race, colour, sex, age, origin, belief, sexual orientation or physical ability.
- Breaching safety rules in a manner that endangers people or Company assets.
- Making an unfounded report in bad faith against an innocent person.
- Consuming, distributing, transporting, selling, and possessing any type of drug.
- Binding the Company legally without the authority or evidence required to do so.
- Omitting or failing to report breaches of the **Code** promptly.
- Carrying out transactions for personal or family benefit, or for the benefit of third parties, to the detriment of the Company.
- Influencing, coercing, manipulating, or deceiving any auditor conducting an investigation or review within the company.
- Distorting accounting records.
- Recording fictitious transactions, including sales, purchases, loans, credit facilities and expenses.
- Cashing cheques using forged endorsements.
- Forging or altering receipts.
- Purchasing unnecessary goods or services to the detriment of the Company.
- Using business email to send bulk mailings.
- Downloading unlicensed software.



Carlos Ricci Voltas

Managing Director

CONCESSIONÀRIA HOSPITAL UNIVERSITARI SON ESPASES, S.A.

Prepared

Name: Marta Pérez

Position: Department of Quality and Environment.

Name: Aina María Guerrero Fullana

Position: Head of Quality, Environment and OHS.

Reviewed

Name: Izaskun Davalillo Peña

Position: Director of HR and Organization

Approved

Name: Carlos Ricci Voltas

Position: General Manager

Name: Criminal Compliance Committee

