Code of Ethics

BlueFloat Energy International, SLU

and

Related Companies

Code of Ethics

Revision to the version approved on 1st June, 2021.

Updated version to the Code of Ethics approved on 24th November 2021.

This Code of Ethics is the property of BlueFloat Energy International, SLU and must be returned if an individual's association with BlueFloat Energy International, SLU or any of its Affiliates[1](*) (collectively referred to as the "**Group**") terminates for any reason. This code of ethics (the "**Code of Ethics**") supersedes previous Codes of Ethics.

[1] Affiliate(s) shall mean: Any Person directly or indirectly controlling, controlled by, or under common control with such Person. For the purposes of this definition, the terms "controlling," "controlled by," or "under common control" means the possession, directly or indirectly, of the power to direct or cause the direction of management or policies (whether through ownership of securities or any partnership or other ownership interest, by contract or otherwise) of a Person.

Section I. Purpose and scope

The Group expects that all its professionals to behave in accordance with the highest ethical standards, respecting the principles and values of this Code of Ethics when conducting their actions. This Code of Ethics is intended to serve as a guide, an informative reference and a documentary source to help all professionals of the Group to choose the most ethically appropriate option in any circumstance.

This Code of Ethics is the backbone document of a Compliance System at the Group that aims to prevent the commission of crimes and other regulatory risks of special relevance to the Group arising from the sector in which it operates.

This document is applicable to all the companies encompassing the Group at any hierarchical level: board of directors, sole directors, senior management, administrative body and other employees (collectively referred to as the "**Code Recipients**").

This Code of Ethics will be applicable to all the Companies of the Group, as well as to those Companies in which it has effective control. In those companies which are minority investments in which the Code is not applicable, the Group will promote principles and guidelines consistent with those established in this Code.

This Code of Ethics shall also apply and govern the Group's relations with respect to third parties, such as customers, suppliers, business partners, public authorities and financial institutions, among others.

Section II. Introduction and applicable regulation

The Group operates globally and partners with other entities on developing and operating joint projects. Our operations subject us to various legal requirements, and we have adopted this Code of Ethics to reflect the principles and values that govern the actions of the Group.

Ethical commitment and regulatory compliance have recently burst onto the business scene. These regulatory changes have set off alarm bells for companies regarding corporate governance.

A legal or regulatory violation could subject the Group to liability and in some cases also subject employees or board members to personal liability. Even an allegation of a violation could seriously damage the Group's reputation. This Code of Ethics must be interpreted and applied together with the behavioral rules already defined by the Group as part of its Compliance System.

The Group undertakes to monitor compliance with laws, rules and decisions from the UN, European Union and any other supranational body applicable to its activities, with specific reference to:

- the principles of the Universal Declaration of Human Rights;
- the fundamental International Labor Organization conventions;
- the principles of the UN Global Compact;
- the principles of the United Nations Convention against Corruption issued in 2003 (the so-called Merida Convention);

- the principles of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions.

All Code Recipients are both entitled and obliged to become familiar this Code of Ethics, contribute actively to its compliance and implementation (including by reporting any breaches).

Each Code Recipient is required to submit annually a certification affirming that he or she has read and understands this Code of Ethics and that he or she will abide by it to the extent applicable to him or her.

Section III. General Compliance

This Code of Ethics provides an introduction to key values and principles that we must follow. You, as a Code Recipient, should use it for guidance to help understand the Group's ethical standards and expectations. However, the Code of Ethics is only a starting point. It does not describe every policy, regulation, or law that may apply.

Answers to ethical questions are not always obvious. When faced with a difficult decision that raises an ethical or compliance issue, ask yourself the following questions:

- Is the action in compliance with this Code of Ethics?
- Is the action legal?
- Is the action in compliance with Group policy?
- How will I feel if I do it?
- Will I be embarrassed or concerned if my conduct is reported in the press or social media or is known by my competitors or supervisors?

If an action or decision is illegal, do not do it. If an action or decision is against this Code of Ethics or any Group policy, do not do it. If an action or decision is inconsistent with the Group's values and principles, do not do it.

If a Code Recipient (i) finds him or herself in an uncertain situation, (ii) discovers any gap or any need for any update or modification of the Code of Ethics, or (iii) discovers any information pertaining to potential violations of the Code of Ethics, you are obliged to consult and/or inform the Group, primarily through the whistleblowing channel established. In addition, Code Recipients are entitled to request explanations in the event of any doubts regarding its application procedures to their immediate supervisor to determine the most appropriate action.

Section IV. Obligations in relation to this Code of Ethics

Code Recipients are required to comply with the following behavioral rules in order to adhere to the general principles and prevent the risk of unethical conduct in the Group:

Lead by Example. ***"Tone from the top".*** Those who supervise others have the additional responsibility of setting an example with their own ethical conduct. Leadership is expected to keep lines of communication open so that employees feel comfortable asking questions and reporting concerns. Leadership is also expected to ensure that employees under their supervision complete assigned training and have adequate

knowledge to follow the principles, values, requirements and expectations established by this Code of Ethics.

Ask Questions. It is our responsibility to ask questions and to immediately bring potential concerns to the Group's attention.

Seek Advice. If you are unsure about the proper course of action, ask your supervisor, or, if your supervisor might be the subject of the concern, speak with a different manager, an officer, or contact the reporting hotline.

Report Concerns. You have a duty to report any concern that is perceived as unethical or in violation of this Code of Ethics, Group policies or legal requirements. If you are aware of suspected misconduct, illegal activities, fraud, misuse of Group assets, or violations of Group policies, then it is your responsibility to report the concern immediately.

No Retaliation. Nothing in this Code of Ethics is designed to prevent an employee from acting in accordance with applicable whistleblower statutes. It is a Group's policy that no employee who submits a complaint made in good faith or reports a violation to a regulatory authority or the relevant Compliance Officer, will experience retaliation or any penalty whatsoever. Any employee who believes he or she has been subject to retaliation or reprisal as a result of reporting a concern or making a complaint is to report such action to the Board of Directors or the sole director. As indicated above, said reports will be processed by the Group in accordance with the action protocol for the management of communications received through the whistleblowing system, set forth below.

Investigations and Consequences of Code of Ethics. When you report a concern, the information will be thoroughly reviewed. If the investigation reveals that a violation of this Code of Ethics occurred, appropriate disciplinary action will be taken, up to and including termination of employment with the Group. Depending on the nature of the violation, other consequences may include reimbursement to the Group for any losses or damages resulting from the violation and/or referral for criminal prosecution.

Section V. Ethical Guidelines

This Code of Ethics prescribes standards of ethical conduct and is binding for all Code Recipients. It is designed to address and avoid potential misconduct and all of them must comply therewith.

Failure to abide by the Code may result in disciplinary sanctions, including termination from the Group.

A. Standards of Conduct

The following basic principles guide all aspects of the Group's business and represent the minimum standards to which the Group expects the Code Recipients to adhere. Therefore, Code Recipients shall

- behave with integrity and treat each other and all persons with whom they interact with respect and equality. In relations with public officials or authorities, special care will be taken, and these will be treated with full objectivity and neutrality;
- comply with all applicable laws complying with national and international regulations on Compliance (e.g. anti-corruption, competition law, environmental law, money laundering, etc.), particularly, those that apply to the Group. In some cases, there may be a conflict between applicable laws in two or more countries, states or provinces. If you encounter a conflict of this type, or if a conflict arises between a local law and a policy described in this Code of Ethics, you should consult your immediate supervisor to determine the most appropriate action;

- advance the legitimate interests of the Group and deal fairly with our customers, vendors, suppliers, competitors and each other;
- not take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair-dealing practice;
- not take inappropriate advantage of their positions of trust with, or responsibilities to, our stakeholders;
- disclose outside business activities, interests, or board memberships, including those of close family members or who maintain bonds of affection or close friendship , that may conflict with the Group's interests or interfere with the employee's ability to exercise his or her duties impartially to their managers in writing;
- protect the confidentiality of information relating to the Group. This applies even when you are no longer a Group employee or are no longer temporarily assigned or working in our offices.

1. Conflicts of Interest

In general, a conflict of interest occurs when a personal or family interest interferes with—or could be perceived to interfere with—our ability to make sound, objective business decisions on behalf of the Group. A conflict of interest or the appearance of a conflict of interest may arise even if you are not in a decision-making role for the Group.

Code Recipients are expected to discuss with their supervisor or the Compliance Committee any practice that creates, or gives the appearance of, a conflict of interest. However, if a Code Recipient is uncomfortable discussing an issue with their supervisor or or the Compliance Committee, or if he or she believes that an issue has not been appropriately addressed, he or she will report the matter to the Board of Directors or the sole director.

Examples of potential conflicts of interest meriting disclosure include (but are not limited to) the following:

- accepting or offering things of significant value (i.e. over EUR 100, preferential loan terms, use of a vacation home, etc.) from or to any vendor, supplier, customer, or competitor of the Group;
- having a personal financial interest in any business transaction in which the Group is involved;
- engaging in any business arrangement or other transaction that conflicts with the interests of the Group;
- personally, accepting business opportunities, commissions, or advantageous financial arrangements from a customer, vendor or business partner; or
- purchasing for personal use goods or services provided by a Group vendor on terms other than those available to the general public or established by Group policy.

You may never take personal advantage of any business or investment opportunity that you may learn about through your work for the Group and that the Group may want to pursue—unless and until the Group has had an opportunity to evaluate it and has chosen not to pursue it. You must not compete with the Group.

2. Diversity and Equal Employment Opportunity

We expect Code Recipients to create and reinforce an inclusive, creative and productive work environment in which everyone feels accepted and respected. At the Group, "diversity" refers to who we are—the various characteristics that make us unique. It includes, among others, age, physical ability, education, religion, ethnic background, sexual orientation, socioeconomic status, race, and gender.

Inclusive behaviors, for illustrative purposes, are the following:

- encourage an understanding of self and others;
- make it safe to talk;
- foster clear two-way communications;
- provide coaching and feedback;
- connect individual jobs to the Group's mission.

Leadership is responsible and accountable for encouraging appropriate workplace behaviors and addressing inappropriate behaviors.

Under no circumstance should any Code Recipient or job applicant be treated more or less favorably because of race, color, ancestry, sex, gender, religion (including religious dress and grooming practices), national origin, age, actual or perceived physical or mental disability, medical condition, genetic information, sexual orientation, gender identity or expression, military or veteran status, marital status, status as a victim of domestic violence, or any other status protected by applicable laws, unless such applicable laws so require. It is your responsibility to report any action that you think is discriminatory.

We are committed to a workplace free from any form of harassment. Harassment undermines the integrity of the employment relationship and respect of human dignity. You have a responsibility to uphold the Group's commitment and report any acts (verbal, physical, or visual) of harassment, intimidation or coercion based on or related to race, color, ancestry, sex, gender, pregnancy, religion (including religious dress and grooming practices), national origin, age, actual or perceived physical or mental disability, medical condition, genetic information, sexual orientation, gender identity or expression, marital status, status as a victim of domestic violence, or any other classification protected by applicable law.

3. Workplace Safety

Our shared commitment to safety is simple: everyone wins when safety comes first.

We have a shared responsibility to resolve unsafe conditions and to maintain a safe work environment for employees, contractors, agents, customers and the general public. We must be mindful of the importance of working in a safety-conscious environment and do our part to keep it that way. We must complete all safety training assigned to us as promptly as possible.

Each of us is responsible—without exception—for reporting promptly any workplace condition that might be unsafe. If you become aware of any workplace injury, you must advise management immediately so that appropriate action can be taken, including documentation of recordable accidents under the applicable law.

One of the many ways the Group ensures that we provide a safe and productive work environment is by requiring all employees to be fit for duty. When issues arise regarding your physical, emotional, or mental

health, ask yourself if you are equipped to work safely. If you believe that you or one of your co-workers is not able to work safely, you should immediately contact your supervisor.

As part of our commitment to safety, we will not tolerate any form of workplace violence. Violence includes any verbal or physical conduct occurring in the workplace or affecting the workplace that causes someone to fear for their personal safety, the safety of co-workers, or the safety of Group property.

If you have knowledge of any workplace violence issue that does not involve imminent danger, contact your supervisor. If you have knowledge of any workplace violence issue that potentially involves imminent danger, contact the police and local authorities.

4. Protection of employee Information

We have an ethical and legal responsibility to preserve the privacy, confidentiality and security of employees´ personal data and personal information, in compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**GDPR**") and the Organic Act 3/2018, of 5 December, on Protection of Personal Data and guarantee of digital rights ("**LOPDGDD**") (jointly GDPR and LOPDGDD referred as the "**Data Protection Regulations**").

4.1. Processing of employee's personal data.

During the course of employment relationships, the Group collects and uses personal data and personal information about employees in accordance with the Data Protection Policy[1] as part of the administration of the employment relationship and, in particular, without being exhaustive, for the following purposes:

- to audit and check the employees' compliance with this Code of Ethics;
- to manage your relationship with the Group and to ensure an adequate maintenance and development of the employment relationship, including, but not limited to, performing absenteeism checks, evaluations, personnel management, absence management, changes of shifts or department, management of form and assistance and use of internal and external courses, training courses, management of business trips and business cards, potential motivational campaigns and benefits aimed at employees linked to performance at work and their time control and attendance;
- to perform our obligations under the employment relationship, the law or other similar regulatory provisions, such as, for example paying your salary, withholding of personal income tax and Social Security contributions, or those derived from the management of work accidents, absences, common casualties and prevention of occupational risks or the obligations under the applicable collective agreement and the employment relationship;
- to professional location purposes when the development of the services under the employment relationship requires for you to contact with clients and providers of the Group;
- to prevent of occupational risks;
- to guarantee the security of the Group's facilities and individuals;
- to subscribe and manage, if voluntarily requested by you, any flexible remuneration scheme and

[1] [1] Data Privacy Policy of Group available in a separate instrument

benefit or compensation plan, including pensions, medical insurance, granted by the Group;

- to execute any mergers, divisions, partial division, transfer of assets and exchange of shares concerning the Group; and
- to contact your dependents and relatives, in case of an emergency and to subscribe the benefits and insurance programs indicated above. When providing the personal data of these dependents and relatives, you confirm that you have informed the abovementioned persons and have obtained their consent for the benefits provided by the Group.

Examples of personal information include data related to contact details and professional career of the employee, including compensation, benefit plan enrollment, performance reviews, phone numbers, home addresses, social security numbers, and other personal data. The processing of your personal data with these purposes can also include the processing of special categories of personal data, mainly concerning health, such as your degree of disability or your aptitude to perform the work or medical leaves, in accordance with and to the extent permitted by Data Protection Regulations in order for us to perform or exercise obligations or rights imposed or conferred by law on us in connection with employment, social security or social protection.

The provision and processing of the personal data is necessary for the execution of the employment relationship and, hence, if you do not provide said data or you request its deletion, the employment agreement cannot be executed. The legal basis for personal data processing is:

- The execution of the employment agreement with the Group.
- The compliance with the obligations imposed to the Group by applicable labor and tax regulations.
- Your consent provided voluntarily to subscribe any of the social benefits and compensation plans, and flexible remuneration scheme offered by the Group;
- Regarding the personal data of your dependents or relatives, the legitimate interest for emergency contact and the consent provided through you to subscribe any of the benefits offered by the Group;

In no case, the Group will carry out any automated decision that may affect you significantly based only on the automated processing of your personal data.

At times, the Group needs to disclose personal information to third parties. The personal data shall only be accessed by:

- to comply with legal and regulatory requirements. European and national regulations govern the disclosure of certain types of personal information to banks, entities collaborating with Social Security and the Tax Administration, or judges and courts;
- vendors that have been contracted to monthly prepare pay sheets and liquidations of social security contributions, provide prevention of occupational risks and medical examinations; accounting and tax management; technical and IT support services; security; audits, consultants and advisors; and training courses providers;
- other companies within the Group, both national and international, detailed in its website https://www.bluefloat.com/, in order to execute the employment agreement, manage human resources overall policies of the group and execute any other aspect of the labour employment at a group level. As long as there are companies of the group located outside the European

Economic Area (EEA), the Group may carry out international data transfers of the personal data to countries where the level of protection of the personal data may not be the same. In those cases, the Group will only carry out those data transfers to countries where the Commission has issued an adequacy decision or, in its absence, when the Group has offered adequate guarantees (model clauses or corporate binding rules), a copy of which you can request in the email below;

- the Group's clients and providers, when it is necessary, only for the professional location of the employees, maintenance of the commercial relationship and execution of the agreements and to provide the employment services; and
- the companies providing the social benefits and retirement plans offered by the Group.

The Group will process your personal data during the employment relationship, or as long as you do not revoke your consent for those purposes where the legal basis is the consent. Upon its termination, or once the consent has been revoked, personal data will be preserved, duly blocked, in order to comply with applicable legal or contractual obligations for the required period of time, which in no case will exceed the period of five (5) years, unless when there is a longer retention period for occupational health.

You and your dependants or relatives may exercise at any moment, according to current Data Protection Regulations, your rights of access, rectification or erasure of data, as well as request a restriction of your personal data processing, your right to object it, or request the portability of your personal data. The concrete right that is intended to be exercised must be clearly expressed and addressed in writing to the Group's via email data.privacy@bluefloat.com. You and your dependants or relatives may also revoke the consent provided, when this is the legal ground to process the personal data, at any time, or submit a claim to the relevant Data Protection Agency.

This information on the processing of the employees' personal data for the employment relationship will also be provided to the employees along with the employment agreement and the Group policies and protocols.

4.2. Processing of other Code Recipients' personal data for the provision of the services

We must be able to trust that anyone who has access to other Code Recipients' personnel records or other personal information in the course of performing their job duties will process the information confidentially and use it only for appropriate business reasons and in compliance with applicable Data Protection Regulations. If you are in a job with the authority to access other Code Recipients' confidential personal information, you must have a legitimate business reason to access the information, and you must not provide this information to anyone inside or outside the Group who does not have a business need to know it. In addition, you must be familiar with the Group's methods of securing personal information when transmitting such information electronically, provide by the Group to all Code Recipients.

4.3. Whistleblowing system

The Group has an internal communication and reporting system (the "**Whistleblowing system**") for Code Recipients to bring to the Group's attention any fact or conduct related to (i) an alleged criminal act or omission or generating a risk of criminal prosecution for or in the Group, or (ii) an alleged non-criminal act or omission within the Group, and (iii) any incident or breach of this Code and any other Group's codes or policies. In an appendix to this Code of Ethics, a full description of the whistleblowing system is included.

All Code Recipients may choose to file any internal complaint by providing his/her contact information or anonymously.

The personal data will be processed by the Group for the purpose of managing, processing and investigating the complaint and taking the appropriate disciplinary or legal measures. The Code Recipient shall have the right to withdraw his/her consent to the processing of his/her name as a complainant with effect for the future at any time and without giving reasons.

Even after the withdrawal, it may be the case that third parties (e.g. authorities or courts) process his or her name. Your withdrawal cannot affect the lawfulness of the processing carried out until you have withdrawn your name, nor can it affect processing for another legal justification (e.g. the public interest described below or the fulfilment of legal obligations).

The Group can also process your personal data when another Code Recipient has filed a compliant about your person. In such case, the Group will only process your personal data for the same purposes of managing and investigating the grounds of the complaint, taking the appropriate disciplinary or legal measures.

The processing of personal data within the framework of the Whistleblower System and this Code is based on the existence of a public interest, under the terms established in Article 6.1.e) of the GDPR, in detecting and preventing claims and the consequent prevention of damage and risks of liability for the Group. Likewise, the Group must comply with the legal obligation to resolve the queries made, applicable by virtue of the provisions of Organic Law 10/1995, of November 23, of the Penal Code, and therefore compliance with the legal obligations of Article 6.1. c of the GDPR may also be the legal basis of the processing. To this end, the processing of the personal data will be strictly necessary to manage the complaint and comply with the aforementioned legal purposes and obligations.

The personal data processed will only be kept for the time strictly necessary to decide on the appropriateness of initiating an investigation into the facts or conduct reported and, once decided, will be deleted from the Whistleblowing System, and may be processed outside the system to investigate the facts for the time necessary to take a decision. Once the investigation of the complaint has been completed and appropriate action has been taken, the data will be kept duly blocked in order to comply with the legal obligations applicable in each case. In any case, the personal data will be deleted from the Whistleblowing System within a maximum period of three (3) months from its introduction in the Whistleblowing System, unless it is kept for an additional period of time because it is necessary to comply with the legal and corporate obligations relating to the operation of the Group's crime prevention model, and it may continue to be processed outside the Whistleblowing System, in the event that the investigation of the Whistleblower has not been completed, for the necessary time.

Personal data would only be processed by the Group and its advisors for these purposes. Code Recipients can exercise their rights under Data Protection Regulations in accordance with the previous section 4.1 of this Code.

5. Involvement in Litigation

Any Group employee must advise your manager immediately if:

- receive any subpoena; or
- are charged with or convicted of or plead guilty or *nolo contendere* (no contest) in a domestic, foreign, or military court to any felony; or
- are charged with or convicted of or plead guilty or *nolo contendere* (no contest) in a domestic, foreign,: investments or an investment-related business, or any fraud, false statements, or

omissions, wrongful taking of property, bribery, perjury, forgery, counterfeiting, extortion, or a conspiracy to commit any of these offenses; or

- are contacted by any regulatory authority or supervisor.

B. Regulatory Requirements

Many aspects of the Group business are subject to regulation by government agencies, energy regulatory bodies, and similar entities in the countries in which we operate. All Code Recipients of the Code are expected to comply with all regulatory requirements applicable to the Group. Accordingly, the record-keeping, monitoring, and safety requirements articulated in this Code of Ethics are necessary to satisfy our obligations under a variety of regulations and laws and must be followed. Beyond the energy regulatory bodies, other government agencies impose and enforce obligations that impact Group's operations. As a result, whenever we conduct our business, irrespective the place the operations are conducted, we must have zero tolerance for corruption, bribery, money-laundering, and other similar illegal and unethical practices, by Group employees, joint venture partners, third party contractors, agents, or customers. We must maintain accurate and complete books and records that transparently and comprehensively describe the nature of every expense and transaction we enter.

1. Commercial Bribery and Kickbacks

The Group prohibits bribery and corruption of any person for any reason. Nothing of value should be promised, offered, or given to any person with whom the Group is doing or is soliciting business, with the intention of obtaining or retaining business or a competitive advantage. Any request for an improper favor, payment, preferential treatment, or other consideration, made in the course of the Group business, must be reported promptly to the Chief Executive Officer.

Code Recipients shall not accept anything of value in connection with any Group business where the item is offered, specifically or generally, in an effort to compromise fair, honest, and transparent business practices. Any such offers must be reported promptly to the Chief Executive Officer.

2. International Business Conduct—Anti-Corruption Compliance

Code Recipients must strictly comply with all laws of each country in which they conduct business considering the provisions of the criminal codes applicable in each country (and with those U.S. laws governing foreign operations such as the Foreign Corrupt Practices Act ("**FCPA**"); laws prohibiting cooperation with foreign boycotts or requiring adherence to country-specific embargoes; and export control laws, the UK Anti-Bribery Act 2010, as framework anti-corruption legislation). Code Recipients also must be respectful and tolerant of the values and customs of the communities and countries in which the Group does business.

In general terms, these legislations make it a crime for companies and their directors, officers, employees, or agents to offer, promise or pay, anything of value—including gifts, payments, investment opportunities, favorably-priced loans, job or internship opportunities, travel, entertainment, or other improper inducements—to a foreign government official (or a member of the official's family) to obtain or retain business or a business advantage for the Group (i.e. to avoid the imposition of a large tax or fine against the Group, to influence an entity to choose the Group as a partner, to obtain confidential information about business opportunities, to obtain a license or other authorization from a government, etc.).

It should be note that "*Government Official*" is broadly defined as, and includes (i) any officer or employee of a government or any government department, agency, or instrumentality, including wholly or partly state-owned or controlled commercial enterprises (i.e. an employee of a state-owned energy company),

or of a public international organization; (ii) any person acting in an official capacity for or on behalf of a government, government entity, stated-owned or controlled commercial enterprise, or public international organization (i.e. multinational banks); (iii) any political party or party official; and (iv) any candidate for foreign political office. Government Officials are not limited to elected officials.

The FCPA, as well as other similar anti-corruption laws enacted in the countries in which the Group does business, prohibit both direct and indirect payments. Thus, the Group can face liability based on improper payments made by its agents or other business partners, including renewable energy developers, equipment and services providers, and joint venture partners, whether or not the Group actually knew of the payments. Accordingly, it is critical that we ensure that the third parties with whom we work understand this prohibition of all corruption or bribery conduct, commit to engaging in business ethically and consistently with this Code of Ethics and with any applicable anti-corruption laws in which the Group operates, and have a strong reputation for engaging in ethical business practices.

The Group must choose its partners and representatives carefully to protect against the business and legal risks of dealing with third parties who do not share our commitment to fair dealing. Prior to entering into an agreement with any agent, consultant, joint venture partner, or other representative who will act on behalf of the Group with regard to any Government Officials or government agencies on business development or retention or on regulatory matters (i.e. customs, permits to operate, etc.), the Group will perform appropriate anti-corruption-related due diligence and impose prudent safeguards against improper payments. Before engaging a third party, you also must review the third-party due diligence questionnaire and third-party red flag checklist. Contracts with representatives who will interact with Government Officials or government agencies must be approved by the Chief Executive Officer.

a. Gifts and Entertainment

No gifts other than the customary business courtesies can be provided to the extent they meet the criteria and approval requirements set forth in this section, but under no circumstances may the purpose of such gift be to receive any preferential treatment in any activity that may be linked to the Group.

Gifts of standard promotional items do not require prior written approval from your supervisor. Standard Group promotional items are: (i) conventional corporate gifts with the Group logo (extraordinary corporate gifts, even with the Group logo, will require pre-approval); and (ii) event tickets (i.e., sporting, cultural, or music tickets and alike) that are regularly purchased by the Group for the use of its customers and employees (special purchases of tickets, however, require pre-approval). The value of a gift and the recipient(s) must be properly recorded in the relevant Group company's books and records.

Meals for Government Officials that do not exceed what is generally considered a reasonable business courtesy do not need prior written approval from your supervisor. Meals for Government Officials that are part of a larger hosting arrangement, entertainment arrangement, or special promotional trip should be included in the request for prior written approval from your supervisor to the extent they are anticipated as part of the itinerary of the hosted officials.

Meals are reasonable when they are limited social invitations and do not carry business obligations or present potential for embarrassment. Generally, meals with a per-person value of less than EUR 100 would be considered reasonable, taking into account the location, context and nature of the event, since what is considered reasonable may vary depending on the circumstances and geographic location; in any other cases, you must obtain pre-approval from your supervisor for any expenses involving Government Officials. A copy of the employee's expense report showing the itemized value of the meal (or other appropriate documentation), as well as the recipients, must be properly recorded in the relevant Group

company's books and records.

This approach allows for the acceptance or giving of promotional gifts, customary business courtesies and token offerings provided all of the following circumstances are present:

- they are directly related to either the promotion, demonstration, or explanation of the Group's capabilities, or the execution or performance of a contract;
- they are reasonable in light of customary gifts and entertainment practices;
- they are provided for a purpose other than to induce the recipient to misuse his/her official position, and under any circumstances, they must not be accepted or given if they may be perceived as intended to influence professional decisions, in view of the timing or for other reasons;
- they must certain not to create the appearance of being an improper payment or a conflict of interest;
- they are legal under the written laws, rules, or regulations of the country (many foreign ministries, agencies, and public international organizations have separate hospitality rules);
- they are not in the form of monetary amounts, securities or items that are readily convertible to cash;
- they must have a fair value. Generally speaking, gifts that do not exceed EUR 100 in value, or the equivalent in the relevant currency, are deemed to have a fair value. When calculating the amount, all gifts and courtesies received from or given to a third party in a six-month period shall be taken into account;
- they cannot be considered inappropriate or unprofessional;
- they are fully disclosed, as appropriate, to the recipient's employer and they are given or received in a transparent manner and, certain cases, they respect commercial practices and generally accepted social courtesy norms; and
- expenses are properly recorded the relevant Group company's books and records. The employee responsible for overseeing the gift or entertainment expense must submit supporting documentation so that the payment or expense is accurately described and reflected in the relevant Group company's books and records.

All Code Recipients should note that the Group reserves the right to prohibit the provision, acceptance, or retention of a gift or offer of entertainment, regardless of value, as it may determine in its sole discretion.

b. Hosting Foreign Officials

On occasion, the Group may receive requests to host Government Officials for training, either at Group facilities or at training opportunities sponsored by outside vendors. Similarly, the Group may be asked to host Government Officials outside of their day-to-day locale at technical or operational committee meetings, other project meetings, or negotiating sessions. These hostings may be required under contractual commitments or requested or offered outside of those commitments.

When these hostings occur outside the Government Official's home locale, extend over more than one day, and involve airfare, hotel, transportation, and meals expenses, these hostings tend to involve more

significant expense amounts. As such, they pose higher anti-corruption and public relations risks than routine hosting and entertainment of Government Officials. Accordingly, the Group's policy is to limit these types of hostings as much as practicable.

In all cases, it is important to ensure that the Group communicates clearly in advance and in writing to the Government Official what expenses will and will not be covered by the Group. Failure to do so can increase legal risks as well as the potential for misunderstandings with the Government Official.

d. Relations with the community

Investments in the community must be transparent and adequately documented as a part of the policy at the Group.

The Group believes in contributing to the communities in which it does business and permits reasonable donations, collaborations and sponsorship (this includes any services rendered as well as the granting of facilities, services or products) to charities and other recipients either ad hoc or under a social investment program.

However, the Group needs to be certain that donations to charities and other recipients are not disguised illegal payments in violation of anti-corruption laws.

The Group also must confirm that the charity or other recipients does not act as a conduit to fund illegal activities in violation of the relevant anti-money laundering regulations or other applicable laws. Accordingly, all charitable donations, collaborations and sponsorships on behalf of the Group must be pre-approved by the Chief Executive Officer, documented and, wherever possible, monitored to ascertain the ultimate purpose or the use made of the contribution.

3. Recordkeeping and Internal Accounting Control Provisions

Group's information must be as reliable as possible, it must comply with applicable legislation and Group rules, and must be diligently safeguarded and archived. No transaction should be mischaracterized or omitted in the relevant Group company's books. Adhering to the Group's internal controls and keeping detailed, accurate descriptions of all payments and expenses is crucial.

Code Recipients must be timely and complete when preparing all reports and records required by the policies of the Group. Where applicable, Code Recipients must obtain all required approvals from their supervisors and, when appropriate, from the relevant governmental entities.

All transactions, income and expenses are to be appropriately accounted for, recognized and documented in their entirety as and when they arise, without omitting, concealing or altering any data or information, such that the accounting and operating records give a true and fair view of the actual situation and can be verified by the control areas and by the internal and external auditors. No undisclosed or unrecorded accounts of Group are to be established for any purpose. False or artificial entries are not to be made in the books and records of the Group for any reason.

Personal funds must not be used to accomplish what is otherwise prohibited by the Group's policy.

The Code Recipients must adhere to the following financial control systems and accounting requirements:

- transactions will be executed in accordance with management's general or specific authorization;
- transactions will be recorded as necessary: (i) to permit preparation of financial statements in conformity with generally accepted accounting principles (GAAP), the International Financial

Reporting Standards (IFRS), or any other criteria applicable to such statements; and (ii) to maintain accountability for assets;

- access to Group assets is permitted only in accordance with management's general or specific authorization; and
- the recorded accountability for corporate assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

Code Recipients shall not make any false or misleading entry in the relevant Group company's books and records for any reason, nor may they engage in any arrangement that results in such prohibited acts. Failure to follow these guidelines could be considered fraud. Evading the Group's internal controls will result in a penalty.

Examples of improper record keeping include: making records appear to show a payment to one person when, in fact, the payment was made to someone else; creating a "slush fund"; submitting false or inaccurate expense account reports; and creating records that inaccurately characterize the true nature of a transaction or payment (for example, reporting an "overhead expense" instead of "commission").

4. Environmental Compliance and Stewardship

Environmental stewardship is embedded in the Group's culture and core values. It is our corporate commitment to conduct our business in an environmentally responsible manner.

Environmental protection is the responsibility of every Code Recipient. We are committed to full compliance with both the letter and the spirit of applicable environmental laws and regulations.

Additionally, Group policies and procedures may be stricter than what other companies mandate, and the Group also may establish best practices that are more rigorous than what our regulators require of us.

Failure to meet our environmental commitments could result in damage to the environment and to the Group's reputation. It also could lead to criminal charges, fines and liabilities and imperil human health and safety.

If you become aware of a situation or practice that you suspect or know is harmful to the environment, or does not comply with the Group's environmental policies or with governing laws, rules and regulations, you have a duty to report your concern to the Group.

5. Antitrust and Fair Competition

We must preserve free and open competition. Our business activities are subject to antitrust laws designed to promote fair competition. The antitrust laws apply to a wide range of activities, including marketing, procurement, contracting, mergers and acquisitions, and the location and operation of our facilities. Antitrust laws are complex, and their requirements are not always obvious. Violations can lead to severe penalties and sanctions.

Ensure that you are dealing fairly, being truthful, and not engaging in any collusive tactics in conducting the Group business. If you have any questions about how antitrust laws may apply to a particular situation, seek advice from your supervisor before taking any action.

6. Insider Information and Trading

Code Recipients are prohibited from trading or "tipping" others who may trade securities while aware of privileged information (commonly referred to as "insider" information) learned in the course of their

business activities in compliance with (i) the Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation); (ii) Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse (market abuse directive); (iii) the Spanish Organic Law 1/2019, of 20 February, of which the Organic Law 10/1995, of 23 November was modified, from the Penal Code, to transpose the European Union's directives[2] in the financial and terrorist sector, and (iv) any other domestic applicable laws.

The Group supports open and fair securities markets because they are key to building trust and investor confidence. Where affected parties and insiders have access to privileged information on the listed companies, as a rule, they cannot:

- prepare or carry out any type of transaction involving the negotiable securities or financial instruments concerned in the privileged information or any other sort of security, financial instrument or contract, whether traded on a secondary market or not, having the negotiable securities or financial instruments concerned in the privileged information as the underlying security;
- disclose the information to third parties other than in the normal performance of their work, profession or office; and
- recommend to a third party that they acquire or assign the securities or instruments concerned or that they cause another person to acquire or assign them based on that information.

The privileged information frequently includes issues such as:

- important corporate transactions (e.g., takeover bids, mergers, capital increase, purchase or sale of stakes in the Group involving change of control or sale of significant corporate assets);
- presentation of financial information or income figures by a listed company that differ significantly from the expected information;
- material changes in the policy for remuneration of the shareholders of a company; and
- information on significant orders for purchase or sale of the Group's securities.

Code Recipient shall not trade in securities of the Group, any Group company, or any other publicly listed company on the basis of insider information obtained while working for the Group.

7. Anti-Money Laundering

Money laundering, terrorism financing and international sanctions pose significant risks from a legal and reputation point of view. The Group as applicable, will undertake enhanced due diligence procedures prior to accepting joint venture partners that the Group believes present high risk of money laundering activities.

Examples, although not comprehensive, of persons posing high risk factors are:

[2] Directive (EU) 2017/1371 of the European Parliament and Council, of 5 July 2017, about the fight against fraud, affecting the financial interests of the EU through Penal Law; and Directive 2017/541/EU of European Parliament and Council, of 15 March 2017, relative to the fight against terrorism.

- persons resident in or organized under the laws of a "non-cooperative jurisdiction" or alike as warranting special measures due to money laundering concerns, and any person whose capital contributions originate from or are routed through certain banking entities organized or chartered in a non-cooperative jurisdiction. For the purposes of this Code of Ethics, "non-cooperative jurisdiction" means jurisdictions included in public lists of high-risk countries. For the determination of countries, territories or jurisdictions of high-risk, the Group shall resort to reliable sources, understanding as such (i) the applicable regulation in force on the matter in the relevant country where the Group operates; (ii) the lists of non-cooperative jurisdictions periodically issued by the Financial Action Task Force (on Money Laundering) (FATF); the Mutual Evaluation Reports on each country issued by FATF or its equivalent regional bodies (GAFILAT, GAFIC, MENAFATF, MONEYVAL and other plurinational institutions), as applicable; or (iii) the reports issued by international bodies or institutions related to each of the above mentioned criteria: World Bank, International Monetary Fund, OECD, European Investment Bank or Inter-American Development Bank
- persons who refuse to give required identifying information;
- persons who wish to make payments in cash, or
- persons who wish to engage in transactions involving foreign shell or offshore companies.

In addition, the Group prohibits doing business with or on behalf of:

- persons and entities on such international, supranational and national lists (in the relevant jurisdiction) as may be promulgated by law or regulations; and
- foreign banks unregulated in the jurisdiction they are domiciled in or which have no physical presence.

As a rule, the Group does not allow cash payments and receipts. Any exception must be duly documented and authorized, be for a small amount, which must in any case be less than EUR 1,000 for payments to third parties, and respect local legislation in force on the matter.

For those jurisdictions and activities in which the Group is subject to supervisory and reporting requirements, the due diligence measures implemented must comply with legal provisions on the matter.

8. Political Contributions

It is strictly prohibited for the Group to make donations or extend loans or advances, either directly or indirectly, whether in their own name or through intermediaries, to public officials or candidates, or to political parties, including candidates, federations, coalitions, temporary electoral formations, foundations and entities related thereto.

9. Treatment of sensitive or confidential information of the Group or third parties

Code Recipients have an obligation to protect and take steps to safeguard confidential and personal information in their possession by collecting and processing data in accordance with applicable laws, professional obligations and our own data management policies and practices.

The disclosure of any confidential and personal information entrusted to us is prohibited unless authorized or required or permitted by law, professional right or duty.

The use of any confidential information about our customers for personal benefit or for the benefit of

third parties is strictly prohibited.

As a rule, any information obtained as a result of the professional relationship with stakeholders should be considered confidential and should be scrupulously avoided, whether personal or commercial, in public or informal conversations with third parties.

Section VI. Acceptable Use of the Group's Computer System

- *Ownership*. Employees have access to the Group's electronic communication system, which includes Group-owned computers, Group-owned telephones, voice mail, facsimile machines, corporate e-mail, intranet, social media pages, and the Internet (the "**Computer System**"). Employees' actions and communications may be attributed to the Group, which could be held responsible for the employees' actions, both on Group-issued systems and devices, as well as on personal devices used for Group business. The Computer System is Group property and it may not be used for illegal or inappropriate uses including downloading inappropriate material, harassment, or offensive communications. All messages, information, and data sent and received by the Computer System are Group property. Incidental and occasional personal use of the Computer System is allowed, along as the frequency and duration of this use is reasonable and does not interfere with the professional services of the employees, being the employee informed that there is no expectation of privacy and that such use will be subject to this policy and any resulting messages and data are the property of the Group. This personal use is allowed when it does not interfere with an employee's work performance, interfere with business operations, individual performance expectations or any other employee's work performance, unduly impact the operation of the Computer System, or violate any other provision of this or any other Group policy.

- *Email Communications*. All employees are reminded that email is considered a business communication and is therefore retained and may be monitored. E-mail communications (addressed to either internal e-mail addresses or external e-mail addresses) are inherently not secure. E-mail information travels through public, unprotected networks prior to being delivered to the recipient. It is at risk of electronic eavesdropping, snooping, and electronic theft. Therefore, employees should use care in drafting and sending e-mail communications.

- *Social Media Communications*. With the exception of factual personal background information, including positions at the Group and prior employers, employees should not conduct Group business or provide any information relating to the Group through social media, except through approved Group social media accounts such as on LinkedIn, and with prior approval from the Chief Executive Officer. Employees must not participate in public discussions of any kind that could be perceived as the expression, on behalf of the Group, of their opinions or views without prior approval from the Chief Executive Officer. This includes discussions on external social networks, enterprise or business forums and other social media.

- *Ephemeral Messaging*. Although the use of ephemeral messaging applications such as WeChat and WhatsApp are becoming more common place, the nature of the messaging renders it difficult to obtain copies of such records should a litigation or government regulatory action so require. Accordingly, ephemeral messaging for Group business should be used sparingly, i.e. to schedule meetings and to confirm delivery schedules, and should not be used for important matters, i.e. to negotiate provisions of a contract, provide approval for expenses, or address red flags in third-party due diligence.

- *No Privacy*. Even though employees have unique user log-in identification codes and passwords to access the Computer System, employees have no expectancy of privacy in the use of any part of the Computer System or in any documents, messages or information created on, with or transmitted over the Computer System. The Group has access to the Computer System and maintains the right to access and monitor, consistent with the law, all documents, messages and information created on, with or transmitted over the Computer System, including e-mail and Internet usage, without further notice to employees, apart from this Code of Ethics. Therefore, the Group reserves the right to monitor individual electronics usage or perform routine systems checks against all the Group issued equipment to ensure compliance with this Code of Ethics and good cybersecurity practices, subject to the requirements of applicable law. Employees are deemed to permit that access and review, provided that the Group will access stored text messages only and strictly when it has a reasonable suspicion that the messages relate to a violation of Group policy or any applicable law and then only as reasonably required for that purpose and in accordance with the proportionality test and applicable laws. All such documents, messages, and information can be reviewed by the Group and law enforcement.

- *Monitoring*. The Group reserves the right to monitor and access the Computer System and all documents, messages or information created on, with or transmitted over the Computer System. These Group rights will be exercised strictly in accordance with applicable law, the Group's business purposes (which include ensuring the appropriate use of the Computer System), and/or in cooperation with requests from law enforcement. The Group also reserves the right to disclose such documents, messages, or information when consistent with the Group's business purposes and with requests from law enforcement.

- *No Offensive Use*. Employees accessing the Computer System are identifiable as "Employees" of the Group. Employees therefore must recognize that they may be viewed as representatives of the Group when they access the Computer System and they must conduct themselves appropriately. Employees may not use the Computer System in an offensive, harassing, illegal, or defamatory manner. This prohibition does not preclude employees protected by the employment applicable regulation that they may have to communicate about working conditions, or in any way limit the rights of those employees. The Group prohibits the use of the Computer System to send or receive offensive or improper messages such as sexually explicit or pornographic messages, images, cartoons or jokes; unwelcome propositions, requests for dates, or love letters; profanity, obscenity, slander, or libel; ethnic, religious, sexual, racial or other slurs; messages containing political beliefs or commentary; or any other message that could be construed as harassment or disparagement of others, to the maximum extent permitted by law.

- *Pornography, Sexually Explicit, and Other Offensive Material*. Viewing, spreading, downloading, or possessing any pornographic, sexually explicit, violent, racist, xenophobic, offensive, in defense of terrorism or, in general, contrary to the law in force or public order or other offensive material on the Computer System is prohibited.*Confidential Information, Solicitation, and Illegal Activities*. Employees may not improperly disclose confidential Group information and materials in any manner, including via the Computer System, unless duly authorized. Nor may Employees use the system to solicit for non-Group commercial activities, religious or political causes, outside organizations, or other non-Group related matters. Employees also may not use the Computer System for illegal activities or purposes.

- *Copyrights, Trademarks, and Patents***.** the Group is aware that intellectual and industrial property is the result of research, development and innovation efforts. Therefore, the Group is committed to

defending these rights, both those that belong to it and those that belong to third parties, including those of its competitors. Employees shall protect and preserve information and technological knowledge by avoiding any misuse that could result in harm to the Group's interests. Moreover, Employees must not violate copyrights, trademarks, or patents. Employees may not copy, download, or use any image, text, video, audio material, software, or other copyright-protected, trademark-protected, or patented data without appropriate authorization. This restriction applies to copying copyrighted, trademarked or patented materials from someone else, the local area networks, or the Internet.

The Group does not grant the employees with any intellectual or industrial right, or trade secret, such as copyrights, trademarks, domain names, patents, designs, utility models, know how, software or other similar rights, except for the limited, nonexclusive and untransferable license of use granted to the employees to use the Computer System and Group goods strictly necessary to provide their services. In any case, the Group may terminate the right of the employee to use all the Computer System and Group's goods.

- *Software*. The Group expressly prohibits the unauthorized use or duplication of copyrighted software. The Group will provide legally acquired software to meet the legitimate Group software needs in a timely fashion and in sufficient quantities for all employees. The Group will comply with all license or purchase terms regulating the use of any software acquired or used by employees. Employees shall not engage in or tolerate the making or using of unauthorized software copies under any circumstances. Employees shall not remove, obscure or alter any copyright or proprietary notices associated with any Group software or related software packaging materials. The Group will enforce reasonable internal controls to prevent the making or using of unauthorized software copies, including reasonable measures to verify compliance with these standards and appropriate disciplinary measures for violation of these standards.

- *Computer System and Data***.** Only Group authorized software and related encryption software tools may be used in connection with the Computer System and all related data. Employees shall not use non-Group licensed or owned software or encryption software tools. The Group prohibits employees from using any software or encryption software tools to access Group data located on the Computer System, unless authorized to do so. Employees shall not disassemble, decompile, reverse engineer or tamper with any software or encryption software tools to prevent the Group from accessing or recovering any and all encrypted information.

- *Right to Search***.** The Group reserves the right to inspect and search all computers, electronic devices, and components of the Computer System, including an employee's personal devices used for Group business. Such inspections and searches will be conducted in accordance with proportionality principle and all applicable laws and under the circumstances indicated in this Code of Ethics.

- *Off-Duty Conduct***.** To the maximum extent permitted by law, any off-duty conduct by an employee must not i) interfere with the employee's ability to perform his or her job effectively; ii) adversely affect productivity and positive interactions in the workplace; iii) contain any ethnic, religious, sexual, racial or other slurs; or iv) utilize the Group equipment or working time to advance non-Group activities. Employees who maintain a web site (other than the Group's website), for example, must not use Group equipment or working time to maintain their web site. Remember that your conduct – even when off duty – reflects on the Group and must comport with the Group's policies.

Section VII. Information Safeguarding

The protection of the Group's confidential information ("GCI") is essential to the Group's capacity to succeed as a business. Those who wrongfully acquire misuse or disclose GCI can cause significant damage and/or losses to the Group.

A "Trade Secret" is information that is economically valuable because it is kept secret and is not easily ascertainable by outsiders to the Group. The holder of a Trade Secret must make reasonable efforts to keep the information secret. In most countries, including Spain, Trade Secrets are subject to specific legal protections. Violations of such laws can result in severe civil and criminal penalties. Such information may not be sold, reproduced, distributed, shared or otherwise used in a manner deemed improper by the Group.

Examples of Trade Secrets include:

- scientific, technical and engineering information such as methods, know-how, formulae, drawings, designs, surveys, data, compositions, processes, discoveries, improvements, inventions, intellectual property development, computer programs and research and development projects, sites and/or business opportunities; and
- financial, technical, business and economic information such as information about business strategies and plans, business opportunities, production and operation costs, marketing strategies, purchasing strategies, profits, sales information, and customer and supplier information including project pipeline development histories, product order histories, project need and preference information, product, site or project development information, product or project delivery schedules, pricing information and lists of customers and suppliers.

Moreover, GCI is other non-public, sensitive information which may not fall within the legal definition of "Trade Secret" but is nonetheless valuable to the Group because it is not known by others and efforts are made by the Group to protect it. GCI includes all non-public information that, if disclosed, might be of use to competitors or investors, or harmful to the Group, its directors, its employees, its stakeholders, its partners, its customers or its suppliers.

During employment and any time after leaving the Group, employees shall not use or disclose any GCI without prior authorization of the Group. It is the responsibility of all employees to surrender any Group records or other GCI upon leaving the employment of the Group, regardless of whether the termination was voluntary or involuntary. Failure to surrender the Group proprietary information upon termination of employment or upon request of the Group at any time may be grounds for legal action.

A. Use of Proprietary Information

Information relating to the general internal business affairs of the organization should be treated as confidential and should not be discussed with anyone inside or outside the organization except on a "need-to-know" basis. Deal or project team members may discuss deals or projects with each other.

All Code Recipients have a responsibility to use this information solely in accordance with performing their job and to avoid unnecessary disclosure of non-confidential internal information about the Group. This responsibility is not intended to impede normal business communications and relationships but is intended to alert Code Recipients to their obligation to use discretion to safeguard internal Group affairs. Code Recipients who have authorized access to confidential information are responsible for its security.

This policy seeks to protect the Group's confidential business information. This policy does not intend to

restrict Code Recipients' right to discuss their wages, hours, and other terms and conditions of employment for their mutual aid or protection.

The foregoing is, in addition to and not in lieu of other obligations that the Code Recipients may be subject to, pursuant to the terms of agreements to which they may be party.

Code Recipients found in violation of this policy are subject to disciplinary action, up to and including termination.

B. Confidentiality Agreements

From time to time, the Group or its affiliates may enter into non-disclosure agreements, also known as confidentiality agreements (each, an "**NDA**"), pursuant to which the Group or its affiliates will agree to maintain the confidentiality of information disclosed to them or their representatives. Code Recipients involved in activities subject to NDAs should ensure compliance with NDAs. The Chief Executive Officer should be made aware of the NDAs to which Code Recipients are subject.

C. Legal Disclaimers

Where necessary, for both internally and externally distributed documents, include prominent disclaimers as applicable (e.g. "PROPRIETARY AND CONFIDENTIAL" or "GROUP CONFIDENTIAL"). Notwithstanding this requirement, unmarked documents and files may still constitute GCI subject to this Policy and must be protected accordingly.

D. Media Inquiries

Code Recipients are prohibited from responding to media inquiries on behalf of the Group unless previously approved by the Chief Executive Officer. All media inquiries should be directed to the Chief Executive Officer.

E. Password Protection

For sensitive information, Code Recipients should undertake efforts to restrict access to electronic files by utilizing passwords. However, Code Recipients should be aware that this safeguard does not provide absolute security, as tools are readily available to "crack" document passwords.

Computer Systems users shall NEVER:

- allow anyone else to use their system privileges;
- share their usernames or passwords with anyone else;
- exceed their authorized access;
- leave their Computer Systems unattended while GCI is accessible; or
- copy or transmit GCI to a non-Group computer system.

Computer System users shall secure their usernames and passwords to prevent unauthorized use and shall properly log out of systems when they have completed use.

Section VIII. Evaluation and monitoring activities

The Compliance Committee shall establish the necessary measures and procedures to monitor, to inform employees and to evaluate the effective compliance with the values, principles of action and rules of conduct contained in this Code of Ethics and related compliance policies.

The Compliance Committee is an internal consultative body responsible for promoting the Group's values and rules of conduct, as well as for monitoring, communicating, disclosing and supervising the Code. The Compliance Committee is also responsible for handling the Complaints Channel, managing and solving doubts, queries and complaints received through the Channel. As part of its commitment to transparency, the Committee maintains a register of its activities and provides answers to internal and external information requests. Regarding the resolution of conflicts, the Compliance Committee acts in an objective and impartial manner, guided by the principle of presumption of innocence. Likewise, it acts in order to guarantee that those employees or third parties who have communicated in good faith any presumed behaviour not compliants with the principles contained in the Code will be protected from any type of retaliation. The "Compliance Committee Statute" defines and governs the functions and standards of the Compliance Committee.

Section IX. Document updates and validity

This Code of Ethics was initially approved by the Sole Director of BlueFloat Energy International, SLU on 1st June 2021. This Code of Ethics is being updated on 24th November 2021. The present update to the Code of Ethichs comes into force on the same date and it is valid until the Sole Director or the Board of Directors, as the case maybe, approves and update, a revision or withdrawal thereof.

This Code of Ethics shall be reviewed and updated in accordance with the rules set forth in the Compliance System of the Group.

Appendixes to the Code of Ethics

- **Appendix I – Compliance Committee**
- **Appendix II - Whistleblowing system: Complaints Channel**
- **Appendix III – Disciplinary System**

Appendix I.- Compliance Committee

The Compliance Committee is an internal consultative body responsible for promoting the Group's values and rules of conduct, as well as for monitoring, communicating, disclosing and supervising the Code of Ethics.

The Compliance Committee is an independent body attributed of powers of initiative and control, legally commissioned for monitoring the effectiveness of the Group's internal control Compliance System. The Compliance Committee will be provided with sufficient resources to perform its functions independently.

The Board of Directors (or the sole director, as the case may be) is responsible for the configuration of the Compliance Committee seeking in all cases to ensure the most suitable arrangement to guarantee the proper representativeness and the effective operations of the Committee. The Compliance Committee will be comprised of a minimum of three members.

Depending on the specific cases, the Compliance Committee may be provided with additional resources, or may request technical or legal support or collaboration from other department or, when necessary, external assessors.

The Compliance Committee is also responsible for handling the Complaints Channel (the "Channel"), managing and solving doubts, queries and complaints received through the Channel.

As part of its commitment to transparency, the Compliance Committee maintains a statistical register of its activities and provides answers to internal and external information requests. A yearly report detailing the level of usage of the Channel by employees, directors, managers and collaborators is issued, although this will not incorporate sensitive or confidential information.

Regarding the resolution of conflicts, the Compliance Committee acts in an objective and impartial manner, guided by the principle of presumption of innocence, also the Group can undertake the necessary steps. Likewise, it acts in order to guarantee that those employees or third parties who have communicated in good faith any presumed behaviour not compliants with the principles contained in the Code will be protected from any type of retaliation.

The "Compliance Committee Statute" defines and governs the functions and standards of the Compliance Committee.

The main responsibilities of the Compliance Committee are:

- Updating, improving and modifing the Code of Ethics.
- Managing the risks found out in the the Compliance System.
- Carriying out an annual plan for the control, supervision and evaluation of the model, monitoring the efectiveness of the control measures implemented.
- Supervising, controlling and assessing the overall functioning of the Compliance System.
- Ensuring the proper management and operation of the mechanisms for reporting

breaches, compliants and queries in the Group (Channel).

- Supporting the governing bodies and management in the decision-making process in the event of potential non-compliance operations.
- Ensuring that all the Group's personnel are properly notified of the controls implemented in the Group and making part of the Compliance System that is applicable to them, as well as of any amendment or update to these ones, and to guarantee that all control owners are notified of the list of controls that are under their responsibility.
- Ensuring adequate training and disclosure to the organisation as a whole with respect to the relevance and importance of the compliance strategy and the Compliance System of the Group and consdering Group's corporate culture.
- Promoting regulatory compliance training activities in coordination with the other areas involved.
- Managing and maintaining the reporting mechanisms set up between the different areas involved in the Compliance System.
- Correcting deviations detected in the accomplishment of the Code of Ethics, to lead by example and to promote consistency in the interpretation and application of the Code of Ethichs worldwide within the Group.
- Regularly (or extraordinarily) inform the Chief Executive Officer of the risk areas that could affect the Group, of the results of the Compliance System's assessment and of the controls and actions plans that have been carried out.
- Informing the President, the Board of Directors or the sole Director of the main compliance issues through regular (or extraordinary) reports.

Appendix II - Whistleblowing system: Complaints Channel

The best manner of preserving trustiness is that in any situation in which personnel have legitimate suspicions that non-compliance conducts have occurred, they are aware that they have a safe, confidential and favourable environment in which they can express their concerns without fear of reprisals.

Users of the Complaints Channel should approach the Compliance Committee through the Complaints Channel available at: https://bluefloat.i2-ethics.com/#/, to inform it of any inappropriate situation or bad practice, query or doubt that should be brought to its attention.

If a person sincerely believes that one of the situations outlined in the Code of Ethics has occurred or could occur, they are asked to put such information in black and white and provide all the evidences in the case. Given that, it is much more difficult, and sometimes impossible, to investigate suspicions communicated in an anonymous manner, all persons are asked, in good faith, to identify themselves in order to begin the investigation of the complaint that will be then anonymized, guaranteeing confidentiality throughout the process.

It is possible, however, that the person may be asked to provide lately further information although it will not be required to participate directly in the investigative process.

The process will ensure the anonymity of the user, security and confidentiality during all phases of the investigation of the complaint as well as non-retaliation.

Nonetheless, no guarantee of total anonymity can be given, as it may be possible that testimony will be required in any resulting internal or external procedures

The person who has expressed their concerns will not be made responsible for their expression nor for not having expressed them earlier whenever it is the case that the person has a legitimate conviction that an inappropriate situation of the type previously mentioned exists. Nonetheless, any accusations expressed maliciously or that lacks foundation will be considered a serious or a very serious infraction of conduct, which could lead to disciplinary action.

The Compliance Committee receives through the Complaints Channel communications about:

- Behaviors not compliants with the Code of Ethics.
- Queries on any issue related to the values of the Code of Ethics.
- Incidents that need to be informed and requests for approval regarding them when necessary.
- Failure to comply with any internal or external regulations.
- Failure to comply with the policies, procedures and protocols of the Compliance System of the Group.
- Detection of possible criminal or fraudulent activities.

The Complaints Channel has different ways of communication accessible to employees at all levels and to third parties. Through these channels, it will be possible to report any query, complaint or incident.

These channels are: PC application, or ordinary mail.

These channels will be available to any employee or third party, and will be disclosed and made known to them in an effective and permanent way to ensure that are accessible and transparent to anyone who wants to use them.

The details regarding the use and operation of the Complaints Channel, minimum content of the complaints and treatment of the information communicated or any other relevant information will be: developed by the internal regulations of the Complaints Channel in order to ensure its correct disclosure, accessibility and knowledge for any potential user, and are currenty available at: https://bluefloat.i2-ethics.com/#/ .

It is expected that those people who subscribe to using these channels of communication have previously and carefully assessed the importance of the matters they wish to raise.

Appendix III - The Disciplinary System

The Group may apply the legal or disciplinary measures considered appropriate under the current legislation, which will be imposed in case of breach of this Code of Ethics or of any of the policies and protocols included in the Compliance System.

Will be considered inappropriate behaviour, and therefore subject to the disciplinary system, not only the act of the person who directly violates the Code of Ethics, but also the behaviour of those who collaborate in such conduct by actions or omission.

No person will be penalized without first giving him the opportunity to present any defence they deems appropriate. A violation or breach of this Code of Ethics that constitutes a violation of the labour regulation will be sanctioned in accordance with current regulations.