ETHICS CHANNEL

Internal Information System Policy

BRUC

INDEX

1. WHAT IS BRUC'S ETHICS CHANNEL?

Bruc Energy, SL and its subsidiaries[1] (**"Bruc"** or the **"Group"**) have a firm commitment to compliance with national and international legislation and business ethics during its business activity, as set out in the Group's Code of Conduct (the **"Code of Conduct"**), which can be consulted at Bruc's website (www.brucmanagementprojects.com).

As part of this commitment, Bruc has implemented an internal information system, articulated around Bruc's Ethics Channel, through which Bruc professionals (as defined below) or any third party must report potential criminal or administrative infringement or any other unlawful conduct, behavior contrary to the Code of Conduct or unethical conduct committed in the context of Bruc's business.

The term **"Bruc Professionals"** includes all persons that make up the Group, including its directors or managers, executives, employees, interns, as well as those natural persons acting on its behalf or representation. In any case, as indicated above, any other natural person who has information about potential wrongdoing in the context of a professional relationship with the Group must use the reporting channel provided for in this Policy. All persons mentioned in this paragraph will be referred to as **"Whistleblower"** or **"Whistleblowers"**.

This policy on the internal information system (the "**Policy**") sets out the main principles of the communications procedure in accordance with the provisions set forth in Law 2/2023 of 20 February on the protection of persons who report violations of the law and the fight against corruption (the **"Law on the Protection of Whistleblowers"**).

As established in article 4 of the Law on the Protection of Whistleblowers, the internal information system regulated in this Policy is the preferred channel for reporting the actions or omissions envisaged for in article 2 of the Law on the Protection of Whistleblower[2]. However, the Law on the Protection of Whistleblowers also establishes an external channel for reporting to the Independent Whistleblower Protection Authority, A.A.I. ("**AIPI**")[3], or the corresponding competent authorities that may be created at regional level, without prejudice to the possibility of also contacting the other competent authorities, depending on the nature of the infringement in question[4].

[1] Group refers jointly to Bruc Energy, S.L. and its subsidiaries under the terms of article 42 of the Commercial Code.

[2] Infringements that may be reported are (i) breaches of EU law when they fall within the scope of Annex I of Directive (EU) 2019/1937 of the Parliament and of the Council of 23 October 2019, affect the financial interests of the Union or affect the internal market; (ii) serious or very serious administrative infringements in accordance with Spanish law; and (iii) criminal offences.

[3] The Law on the Protection of Whistleblowers authorizes the creation of the AIPI, although this authority has not yet been created as of the approval date of this Policy.

[4] Depending on the information in question, communications may be addressed to different authorities including the National Markets and Competition Commission, the State Tax Administration Agency, the National Securities Market Commission, the Spanish Data Protection Agency, etc. or, where appropriate, the competent criminal authorities (Criminal Investigating Court or Justice of the Peace, Security Forces or Corps of the State, the Autonomous Communities or the Local Corporations, and the Public Prosecutor's Office or, when the facts potentially entail a criminal offence affecting the financial interests of the European Union, the European Public Prosecutor's Office).

2. MEANS OF SUBMITTING COMMUNICATIONS

Bruc's internal information system includes the following channels for the submission of communications:

(i). In writing:

a. Through the **digital Ethics Channel** that Bruc has in place. This channel can be accessed here.

b. By **post** addressed to the Responsible of the System[5], to be sent it to the following address: Arturo Soria 336, 7 izquierda, 28033, Madrid.

(ii). Verbally:

a. Through the **digital Ethics Channel** that Bruc has in place, by recording a voice message or making a telephone call. This channel can be accessed here.

b. By **calling** the Responsible of the System to +34 910492775.

c. At the request of the Whistleblower, by means of a **face-to-face meeting** with the Responsible of the System within seven days of receiving the request.

If the facts disclosed in the communication involve the Responsible of the System, the Whistleblower may submit the communication directly to Bruc's CEO. The Whistleblower may send his/her report to the CEO (i) in person, (ii) by telephone call, +34 910492775; (iii) by post, Arturo Soria 336, 7 izquierda, 28033, Madrid.

3. PRINCIPLES OF THE INTERNAL INFORMATION SYSTEM

3.1 CONFIDENTIALITY

Any person who directly or indirectly participates in the processing of communications and the corresponding internal investigations must respect the confidentiality of both the received communication and the investigation carried out, in accordance with the applicable legislation. If a communication is made via a channel other than those mentioned in this Policy and is sent to any Bruc Professional, the Group Professional receiving the communication must immediately forward it to the Responsible of the System and is also subject to the aforementioned confidentiality obligation.

The guarantee of confidentiality of the Whistleblower's identity is one of the internal information system's guiding principles. Therefore, Whistleblower's data will not be disclosed to any persons other than those involved in the receipt and processing of the communications or, when appropriate, in the assessment and implementation of any corrective, legal or disciplinary measures that may be

[5] As defined in section 3.5 of the Policy.

considered necessary. The Whistleblower's identity will not be disclosed to the investigated party, nor shall any personal data that indirectly allows the Whistleblower's identification to be disclosed.

3.2 RIGHT TO ANONYMITY

The Ethics Channel regulated in this Policy allows anonymous communications, regardless of the means by which communications are made (verbal or written). However, Bruc encourages Whistleblowers to disclose their identities, to the extent that this facilitates the respective investigation proceedings.

3.3 PROHIBITION OF RETALIATIONS

The Whistleblower acting in good faith may not be penalized or suffer any negative consequences or retaliations[6] (including threats or attempts thereof) for having submitted a report. This non-retaliation guarantee extends to individuals and legal entities related to the Whistleblower[7], to the individuals who, within the organization in which the Whistleblower provides services, assist the Whistleblower in the process and to the legal representatives of the employees in the exercise of their functions of advising and supporting the Whistleblower. Merely cooperating with the investigation must never be grounds for sanction, retaliation or any other negative consequence.

Communications with information known to be false or without reasonable grounds to believe that it is true at the time the communication is made are strictly prohibited. Whistleblower protection shall not apply in such cases and the Whistleblower shall be subject to disciplinary sanction (including disciplinary dismissal) and, as the case may be, to the administrative, criminal and/or civil responsibilities criminal and/or civil liabilities provided for in the applicable regulations.

3.4 RIGHTS OF THE INVESTIGATED PARTY

The investigated party is entitled to be informed of the actions or omissions attributed to them and to be heard by the internal investigator as many times as requested. However, communications with the investigated party will be held at the time and in the manner considered appropriate to ensure

[6] In accordance with article 36(2) Law on the Protection of Whistleblowers, the general concept of retaliation includes "*any acts or omissions that are prohibited by law, or that, directly or indirectly, entail unfavourable treatment that places people who suffer them at a particular disadvantage compared to another in the employment or professional context, due exclusively to their status as whistleblowers, or because they have made a public disclosure*". Furthermore, in accordance with article 36(1) Law on the Protection of Whistleblowers, all acts amounting to retaliation are prohibited, including both threatened and attempted retaliation.

[7] Specifically: (a) individuals who are related to the Whistleblower and who may suffer retaliation, such as co-workers or family members of the Whistleblower; and (b) legal entities, for whom the Whistleblower works or with whom they have any other relationship in an employment context or in which they have a significant shareholding. For these purposes, a stake in the capital or in the voting rights over shares or holdings is considered to be significant when, due to its size, it enables the person who holds it to have the capacity to influence the legal entity in which the stake is held.

the successful outcome of the investigation and must be conducted in compliance with the confidentiality guarantee. During the internal investigation, it will be respected the investigated party's right to defend their interests, the right to defense, to honor and other rights provided for in the applicable regulations.

3.5 EFFECTIVE PROCESSING OF COMMUNICATIONS

Bruc's Head of ESG is the person responsible for managing the internal information system regulated in this Policy, in accordance with the provisions set forth in article 8 of the Law on the Protection of Whistleblowers (the "**Responsible of the System**" or the "**Responsible**").

The Responsible of the System will be responsible for ensuring the effective implementation of the Ethics Channel and this internal information system, and the diligent handling of communications, acting with the utmost confidentiality and independently and autonomously from the rest of the internal bodies and having all the necessary personal and material resources for this purpose.

The Responsible of the System will admit the communication for processing unless any of the following circumstances arise:

(i). where the facts communicated are completely implausible;

(ii). where the facts do not relate to the possible perpetration of a criminal offense or administrative infringement or any other unlawful conduct or behavior contrary to the Group's Code of Conduct committed within the context of the Group's activity;

(iii). when the communication is clearly groundless (e.g. where it is based on mere personal opinion without any indication of veracity) or there are reasonable grounds to believe that the information supporting the communication has been obtained as a result of a criminal offence; and

(iv). when the communication relates to facts covered by a previous communication and does not contain significant new information justifying its processing.

Without prejudice to the decision on the admissibility of the communication, an acknowledgement of receipt of the communication will be sent to the Whistleblower within seven calendar days of receipt, unless this could jeopardize the confidentiality of the information.

Communication with the Whistleblower is permitted and, if considered necessary, additional information on the communicated facts may be requested from them. Accordingly, the Whistleblower may provide an address, email address or safe place to receive the corresponding communications.

The communications admitted for processing will be handled effectively and studied in detail in order to adopt the measures that, where appropriate, are considered pertinent.

The Responsible of the System will ensure that there are no current or potential conflicts of interest in the processing of communications in order to ensure that they are handled with the utmost impartiality and objectivity.

In the event that the communication refers to the Responsible of the System or involves the Responsible of the System, he/she shall refrain from participating in its investigation and immediately inform the CEO of the Company, who will proceed with the investigation.

The maximum timeframe for providing feedback to the Whistleblower on the investigation is set at three months from the receipt of the corresponding communication, excluding cases of special complexity that require an extension, in which case the period may be extended by up to three additional months.

3.6 INVESTIGATION AND CONCLUSIONS

In the event that the communication is admitted for processing, the Responsible of the System will be the instructor and, therefore, the person in charge of carrying out an investigation adapted to the complexity and circumstances of the case to verify the veracity of the facts reported.

In the event that the person under investigation is the Responsible of the System or that the Responsible of the System may have a conflict of interest in relation to the facts under investigation, Bruc's CEO will appoint a substitute instructor to carry out the investigation without the Responsible of the System being able to intervene in it.

The instructor will manage the practice of all the investigation proceedings that are appropriate for the clarification of the facts. These diligences may consist of:

i. conducting interviews with the person under investigation or with other persons;

ii. requesting information and documentation from third parties;

iii. collecting all the information or documentation it deems necessary from any person who is part of Bruc;

iv. requesting the support of external experts for the analysis of certain information or documentation; and

v. any other procedure that the investigator deems appropriate for the investigation of the facts and that complies with the applicable regulations and the provisions of this Policy.

In the event that the facts under investigation are already being investigated by the competent authority, the investigator shall take this circumstance into account when assessing the appropriateness of carrying out the investigative measures indicated in this section.

Once the investigation has been carried out in each case, the investigator shall issue a report indicating the actions carried out, as well as the conclusions reached. This report shall be sent to Bruc's Audit Committee.

Notwithstanding the foregoing, the Responsible of the System may periodically inform the Audit Committee and/or the Board of Directors of the communications received, and the progress made in its processing.

4. DATA PROTECTION

4.1 DATA CONTROLLER

Bruc, as the matrix of Bruc's Group, will be consider responsible for the processing of personal data derived from the use of the internal information system and the processing of internal investigations (the "**Personal Data**") in accordance with this Policy and with the provisions of the legislation on personal data protection. Each entity of Bruc's Group, or any person involved in the internal investigation or involved in the processing of personal data derived from the use of the internal information system and the processing of internal investigations shall be considered co responsible of the Personal Data.

The Data Protection Officer is the point of contact with Bruc and with the different companies of the Bruc Group as co-controller entities for the processing of Personal Data. If they wish, data subjects may contact the Data Protection Officer at the following e-mail address protecciondedatos@brucmanagement.com.

4.2 PERSONAL DATA CATEGORIES AND SOURCES OF DATA

The Personal Data that will be processed within the scope of the internal information system will be identification, contact, economic, professional and employment data and those relating to the facts communicated, and on exceptional occasions when necessary in the context and in accordance with the nature of the investigation, special category data (including data relating to criminal or administrative offences, health, sexuality, or ethnic or racial origin), as well as any other data derived from the use and operation of the communication channel regulated in this Policy.

Personal Data processed within the scope of the internal information system will be those provided directly by the data subjects or, as the case may be, by the Whistleblowers, as well as by Bruc Professionals and third parties from whom information is requested in the course of the investigation, if any, and which in all cases will be related to the facts investigated.

4.3 PROCESSING OF PERSONAL DATA (PURPOSES, LEGAL BASIS AND STORAGE PERIODS)

4.3.1 Purposes of the processing and basis of the internal information system

Personal Data will be processed for the purpose of managing communications and deciding on whether or not to admit them, and, if admitted, to carry out the corresponding investigation and to take any corrective and disciplinary measures that may be appropriate.

Data processing will be conducted on the basis of the fulfilment of the Group's legal obligations —article 6(1)(c) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (**"GDPR"**)— or, where applicable, the fulfilment of a task carried out in the public interest —article 6(1)(e) of the GDPR— in accordance with the Law on the Protection of Whistleblowers.

Similarly, and only when strictly necessary for these purposes, special categories of data may be processed for reasons of substantial public interest in accordance with Article 9(2)(g) of the GDPR.

4.3.2 Storage of data in the internal information system

Personal Data will only be processed in the whistleblower channel for the time required to take a decision on their admissibility and will not be disclosed to third parties, unless necessary for the proper functioning of the system or for deciding on the admissibility of a communication.

In particular, when communications are submitted verbally, the Whistleblower acknowledges that the communication will be documented (i) by recording the conversation in a secure, lasting and accessible format; or (ii) through a complete and accurate transcription of the conversation performed by the personnel responsible for processing it, in which case the Whistleblower will be offered the opportunity to check, rectify and accept by signing the transcription of the conversation.

Once the admissibility or inadmissibility has been decided, the Personal Data will be erased from the whistleblowing channel and, in any case, if no decision has been taken in this respect, three months after its registration. However, a limited amount of information may be stored for a longer period of time to provide proof of the system's operation.

4.3.3 Processing of internal investigation and subsequent storage of data

If the communication is admitted for processing, the Personal Data may be processed outside the whistleblowing channel by the investigation team to carry out the relevant internal investigation. This processing will be conducted in compliance with the Group's legal obligations —art. 6(1)(c) GDPR— or, where applicable, compliance with a mission in the public interest —art. 6(1)(e) GDPR— in accordance with the Law on the Protection of Whistleblowers.

Personal Data will be processed for the time necessary to complete the investigation and to comply with legal obligations.

If the information provided or any part of it is found to be untrue, it must be immediately deleted as soon as this is known, unless the untruthfulness could amount to a criminal offence, in which case the information will be kept for the time required for the legal proceedings.

Once the investigation is complete, the Personal Data will be stored for the time necessary to take and implement the appropriate measures and, subsequently, for the maximum limitation period of any legal or contractual actions. In no case will the data be stored for more than ten years.

4.3.4 Recipients of the data and international transfers

Personal Data will be processed by the Responsible of the System and those persons within the Group who, in the scope of their authority and duties and in accordance with the Law on the Protection of Whistleblowers, are required to do so. It will only be disclosed to third parties when appropriate for the investigation (e.g. service providers or external consultants) or for subsequent corrective action (e.g. the head of human resources —when disciplinary action is to be taken against an employee— or the head of legal services —when legal action is appropriate in connection with the facts communicated— of the Group).

The Whistleblower's identity may be disclosed to judicial authorities, the Public Prosecutor's Office or the competent administrative authorities in the context of a criminal, disciplinary or sanctioning investigation. Disclosures made for these purposes will be subject to the safeguards set out in the applicable legislation. In particular, the Whistleblower will be informed of this before his/her identity is disclosed, unless such information could jeopardize the investigation or the judicial proceedings.

If the facts communicated or subsequently investigated involve circumstances requiring an international transfer of Personal Data, appropriate measures will be taken in accordance with the applicable legislation. Likewise, if the processing of data by any of the service providers assisting in the management of the whistleblowing channel or the investigation involve international transfers, these will be carried out in accordance with the applicable legislation. For example, standard contractual clauses approved by the European Commission will be adopted or Personal Data will be transferred to countries for which the European Commission has recognized that they provide an adequate level of Personal data protection (e.g. the United Kingdom or Japan). Information on the safeguards taken by Bruc Group may be requested by contacting the Data Protection Officer.

4.3.5 Exercise of personal data protection rights

Data subjects may contact the Responsible of the System or the Data Protection Officer for the purpose of exercising their rights of access, rectification, objection, erasure, portability, restriction or any other rights recognized by law in relation to the data appearing in the corresponding file, in accordance with the applicable legislation. However, when the person to whom the facts are attributed or any third party exercises his/her right of access, the Whistleblower's identification data will not be disclosed to them.

Data subjects may also file a claim or request related to the protection of their Personal Data with the corresponding Data Protection Authority, in Spain, the Spanish Data Protection Agency (www.aepd.es).

4.3.6 Obligations of the Responsible of the System

The Responsible of the System will ensure that a logbook is kept of the communications received and the internal investigations to which they give rise, guaranteeing the confidentiality requirements and the data protection obligations provided for in this Policy and in the applicable legislation. In

particular, access to all or part of the contents of this logbook may be granted by virtue of a judicial order issued within the context of a judicial proceeding.

5. TRAINING AND DISSEMINATION

The content of this Policy, as well as the operating of the Ethics Channel, will be the subject of all communication and training actions required for its knowledge and understanding.

Likewise, a copy of the Policy will be sent to Bruc Professionals when joining any of the Group's companies. In addition, the Group's website will include a specific section on the existence of the Ethics Channel in which this Policy will be published.

6. APPLICABLE LOCAL LEGISLATION

This Policy has been created based on the applicable Spanish legislation (in particular, the Law on the Protection of Whistleblowers), as well as the principles and obligations set forth in Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union Law. In case the communication is subject to any other country's legislation, the Policy shall be applicable without prejudice to compliance with legislation other than Spanish legislation (within its scope of application) to the extent that such legislation sets forth additional protections or guarantees to those provided for therein.

7. DISCIPLINARY REGIME

Breach of the provisions of this Policy may give rise to disciplinary sanctions or other appropriate action depending on the offender's relationship with Bruc Group.

8. RELEASE AND COMING INTO EFFECT

Bruc's Board of Directors is responsible for approving this Policy and its subsequent revisions.

The Policy applies to the Group under the terms set forth in Article 11 of the Spanish Law on the Protection of Whistleblowers.

Date of update: June 18, 2024

***