GENERAL INFORMATION SECURITY POLICY

BRUC

Confidential

Content

1. INTRODUCTION 3
2. SCOPE OF APPLICATION 3
3. SECURITY APPROACH 4
4. GENERAL PRINCIPLES 4
5. THE ROL OF THE BOARD OF DIRECTORS 4
6. STRATEGIC OBJECTIVES 5
7. RISK MANAGEMENT FRAMEWORK 5
8. GOVERNANCE, ROLES AND RESPONSABILITIES 5
9. THIRD-PARTY AND SUPPLY CHAIN MANAGEMENT 6
10. AWARENESS, TRAINING AND DUTY OF COOPERATION 6
11. INFORMATION SECURITY REGULATORY FRAMEWORK 7
12. SECURITY AND RESILIENCE MANAGEMENT SYSTEMS 7
13. NON-COMPLIANCE 8
14. ETHICS CHANNEL 8
15. APPROVAL AND ENTRY INTO FORCE 8

1. INTRODUCTION

Bruc Energy, S.L. and the companies within its corporate group ("BRUC" or the "Group"), are aware that information constitutes a strategic asset essential for the development of its activities and the secure delivery of its services, and promote a comprehensive information security management approach based on risk analysis and treatment, in line with the principles and requirements established by recognized standards and reference frameworks, including ISO/IEC 27001, the Spanish National Security Framework (ENS), and Directive (EU) 2022/2555 (NIS2), as well as in compliance with BRUC's Code of Conduct and all other applicable corporate rules and policies.

For this reason, BRUC publishes this General Information Security Policy (hereinafter the "GISP" or the "Policy"), which establishes the principles, criteria, responsibilities, and corporate guidelines governing the protection of information, the assets supporting it, and the services dependent on information and operational technologies within BRUC.

The GISP constitutes the governing reference framework for defining, implementing, maintaining, monitoring, and continuously improving the technical, organizational, physical, and documentary measures necessary to protect information and the systems that handle, store, transmit, or process it, in accordance with a comprehensive risk-based approach, business needs, applicable legal, regulatory, contractual, and sector-specific requirements, and recognized best practices in information security, business continuity, and operational resilience.

This Policy is aimed at ensuring an adequate and proportionate level of protection for information and for the services that are essential or relevant to BRUC's activities, ensuring the capability to prevent, detect, respond to, recover from, and learn from incidents or situations that may affect information security, operational continuity, or regulatory compliance.

2. SCOPE OF APPLICATION

The Policy applies to all companies forming part of the Group, as well as to non-Group affiliated companies over which BRUC exercises effective control, within the limits established by applicable law. In those affiliated companies where this Policy does not apply, BRUC shall promote, through its representatives on their governing bodies, the alignment of their own policies with this Policy. Furthermore, this Policy shall apply, where appropriate, to joint ventures, temporary business associations, and other equivalent arrangements where BRUC has management responsibility.

The GISP also applies to all employees maintaining an employment relationship with BRUC (the "Professional" or the "Professionals"), as well as to directors, temporary staff, interns, collaborators, suppliers, contractors, subcontractors, clients, and any third party who, with or without an employment relationship with BRUC, have access to information, assets, systems, or services under the Group's responsibility. Likewise, it applies to all areas, functions, processes, activities, facilities, assets, systems, networks, platforms, and services owned, managed, operated, controlled, or otherwise under the responsibility of BRUC, regardless of their geographical location or service delivery model.

Its scope includes, among others, IT and OT environments, cloud environments, corporate networks, communications infrastructures, physical facilities, outsourced services, third-party technological solutions, and any other medium or support involved in the information lifecycle.

Any subsidiaries, branches, energy plants, operational centers, or organizational units that, due to local, operational, regulatory, or contractual requirements, develop specific regulations or procedures, shall ensure that such regulations or procedures are aligned with this Policy and with the regulatory framework implementing it. In the event of any discrepancy, the provisions of the GISP and the corporate regulations shall prevail, unless local regulations establish more stringent requirements.

3. SECURITY APPROACH

Information is an essential asset for BRUC and must be protected throughout its entire lifecycle, from its creation or receipt to its destruction or permanent retention, through controls that are appropriate and proportionate to its criticality, sensitivity, business value, legal obligations, and associated level of risk.

BRUC adopts a comprehensive, continuous, cross-functional, and risk-based security approach, whereby information security is integrated into business processes, operational management, corporate governance, change management, third-party contracting, and decision-making processes relevant to the Group.

Information security is a shared responsibility. All individuals subject to this Policy must be aware of, accept, and comply with the security obligations applicable to them, use the assets and resources made available to them diligently, and actively collaborate in the prevention, detection, and reporting of risks, vulnerabilities, and incidents. BRUC may monitor, log and review the use of its systems, networks and information assets, as well as user activities, for security, operational resilience, compliance and incident management purposes, in accordance with applicable laws and regulations.

4. GENERAL PRINCIPLES

BRUC conducts its information security activities in accordance with the following principles:

- **Confidentiality:** ensuring that information is accessible only to authorized persons or systems.
- **Integrity:** ensuring that information is complete, accurate, and has not been altered in an unauthorized manner.
- **Availability:** ensuring that information and systems are accessible when required by authorized users.
- **Authenticity:** ensuring that the identities of users, systems, and data are genuine and verifiable.
- **Traceability:** the capability to record and trace actions performed on information for subsequent analysis or audit purposes.
- **Retention:** ensuring that information is maintained and protected for the necessary period of time, in compliance with legal and operational requirements.
- **Proportionality:** applying security measures commensurate with the level of risk, avoiding excessive or insufficient controls.
- **Risk management:** identifying, analyzing, assessing, and treating risks affecting information.
- **Security by design and by default:** integrating security from the conception of systems and processes, applying secure configurations by default.
- **Continuous improvement:** ongoing review and updating of security measures to adapt to new threats and evolving needs.

The interpretation and implementation of these principles shall be carried out through the specific regulations forming part of BRUC's information security regulatory framework.

5. THE ROLE OF THE BOARD OF DIRECTORS

The Board of Directors of BRUC expressly undertakes to promote, approve, support, and oversee this Policy and the regulatory framework implementing it, fostering a security culture aligned with the Group's strategy, business model, and risk profile.

The Board of Directors is responsible for ensuring that information security is supported by appropriate governance, sufficient resources, clearly defined responsibilities, and effective monitoring and control mechanisms, as well as for periodically reviewing its effectiveness and promoting any necessary improvement actions.

To this end, BRUC shall promote the necessary training and awareness of the members of the Board of Directors and personnel with relevant responsibilities in the areas of security, technology, business continuity, operations, control, procurement, and third-party management.

6. STRATEGIC OBJECTIVES

This Policy pursues, as strategic objectives, the comprehensive protection of BRUC's information, technological assets, operational assets, and services against internal and external threats, whether deliberate or accidental; ensuring the continuity and resilience of critical or relevant processes and services; aligning security with the business and technology strategy; and establishing and maintaining an effective framework for managing information security, cybersecurity, continuity, and third-party risks.

Likewise, the Policy aims to prevent, detect, manage, respond to, and recover effectively from incidents; comply with applicable legal, regulatory, contractual, and sector-specific requirements; strengthen security within the supply chain and third-party relationships; integrate security into the processes of acquisition, design, development, implementation, maintenance, and decommissioning of systems; promote a security culture; ensure segregation of duties; and maintain monitoring, oversight, auditing, and continuous improvement capabilities.

7. RISK MANAGEMENT FRAMEWORK

BRUC establishes an information security and cybersecurity risk management framework that enables the systematic identification, analysis, assessment, treatment, acceptance, monitoring, review, and escalation of risks that may affect information, the assets supporting it, and the continuity of services.

This framework shall encompass, at a minimum, technological, operational, physical, environmental, organizational, legal, regulatory, third-party, supply chain, outsourced services, cloud environment, and operational or industrial systems risks applicable to BRUC.

The methodologies, assessment criteria, acceptance levels, responsibilities, frequencies, tools, and mechanisms for risk monitoring and reporting shall be developed through the corresponding corporate regulations and procedures, which shall form part of BRUC's information security regulatory framework.

8. GOVERNANCE, ROLES AND RESPONSABILITIES

Information security is structured in accordance with a governance model that ensures the proper segregation of duties, coordination among areas, clear assignment of responsibilities, and independent oversight of the control framework.

Without prejudice to the level of detail established in the implementing regulations, BRUC adopts a responsibility model based on three lines of defense, under the supervision of the Board of Directors as the highest governing and oversight body.

1. **The first line of defense** consists of the business units and support areas responsible for operating the processes, services, assets, and controls within their scope of responsibility. These functions are responsible for applying the established security measures, identifying and managing the risks associated with their activities, escalating significant deviations, and reporting incidents, vulnerabilities, or non-compliance situations that may affect information security.

2. **The second line of defense** consists of the corporate functions responsible for defining, supervising, controlling, ensuring compliance with, and monitoring the information security and cybersecurity framework. These functions operate with the degree of independence required from day-to-day operations, establishing criteria, methodologies, requirements, monitoring mechanisms, and validation processes to verify compliance with the internal and external regulatory framework, as well as escalating identified deviations, risks, or deficiencies to the appropriate governing bodies.
3. **The third line of defense** corresponds to Internal Control or any independent function designated by BRUC, provided that it operates with sufficient independence from ordinary management and oversight functions. This third line provides an independent and objective review of the effectiveness of the governance model, the management system, internal control, and risk management relating to information security and cybersecurity.

The Board of Directors, as the highest governing and oversight body, holds ultimate responsibility for information security and cybersecurity matters. In this regard, it is responsible for defining and/or approving, as appropriate, the strategic framework, the general security principles, and the Group's risk appetite, ensuring the existence of adequate policies, controls, capabilities, and resources. Likewise, it oversees the proper management of significant risks and ensures that Senior Management promotes effective measures to prevent, detect, respond to, and recover from security incidents.

Additionally, BRUC has a Security Committee, understood as the internal body responsible for the coordination, monitoring, prioritization, reporting and escalation of relevant information security and cybersecurity matters. This Committee operates in accordance with its internal regulations, which govern, among other aspects, its composition, meeting frequency, responsibilities, decision-making mechanisms, and escalation channels.

9. THIRD-PARTY AND SUPPLY CHAIN MANAGEMENT

BRUC requires third parties with whom it engages, where such engagement involves access to information, systems, assets, facilities, networks, or services under its responsibility, to implement security measures that are appropriate and proportionate to the level of risk. These measures shall be formalized through contractual requirements, vendor qualification controls, assessment processes, monitoring mechanisms, and, where appropriate, verification or audit rights.

The management of third-party and supply chain risks shall address, among other aspects, the classification of services, the criticality of the supplier, the degree of operational dependency, the handling of information, subcontracting processes, incident notification obligations, service continuity, reversibility or orderly exit arrangements, and the protection of BRUC's assets throughout the duration of the contractual relationship.

10. AWARENESS, TRAINING AND DUTY OF COOPERATION

BRUC promotes a corporate security culture through ongoing awareness, training, and educational programs tailored to the risk profile, level of responsibility, and functions performed by the different groups subject to this Policy.

In this regard, BRUC establishes and maintains awareness, training, and educational activities in the fields of information security, cybersecurity, and risk management, aimed at its professionals, directors, and other groups included within the scope of this Policy, in a manner proportionate to their functions, responsibilities, and exposure to risk. These activities are intended to ensure an adequate level of understanding of the applicable obligations, promote secure behaviors, and reinforce the adoption of best practices in the use, handling, and protection of information and associated assets.

Every person included within the scope of the GISP has the duty to act diligently, protect the BRUC assets to which they have access, comply with the applicable rules and instructions,

promptly report any security weakness, non-compliance, or incident of which they become aware, and cooperate in any investigations, verifications, and response measures that may be necessary.

11. INFORMATION SECURITY REGULATORY FRAMEWORK

This GISP is implemented through a hierarchically structured corporate information security regulatory framework, which enables the principles and mandates of this Policy to be translated into provisions with greater detail, control, and operational effectiveness. This framework shall be aligned with the ENS and other applicable regulatory requirements. In particular, the documents comprising Levels 2 to 4 shall develop and implement the security measures and minimum controls applicable to BRUC, including those established in Annex II of the ENS, taking into account the categorisation of information systems according to their impact on confidentiality, integrity, availability, authenticity and traceability.

This regulatory framework is organized into different levels, defined according to their scope, purpose, and degree of specificity:

Level 1 - General Information Security Policy (GISP):
This constitutes the highest-level framework of the information security regulatory framework, upon which all documents forming part of it depend. It is a strategic document that formally establishes and presents, at a high level, the principles, guidelines, and commitments relating to information security.

Level 2 - General Policies (GP):
These develop the principles established in the GISP by setting out the foundations of the different security domains. These policies define the framework for action and guide the drafting of the lower-level Standards, grouping and structuring the various security areas.

Level 3 - Standards:
These specifically establish the controls, requirements, and guidelines that must be applied to ensure the adequate protection of information assets. Each Standard is aligned with a General Policy and is defined considering the applicable security domains and regulations.

Level 4 - Procedures and Supporting Documentation:
This includes procedures, technical instructions, guidelines, directives, annexes, and other operational documents, whose purpose is to detail the practical implementation of the controls and guidelines defined at the higher levels, as well as to generate the corresponding records and evidence.

12. SECURITY AND RESILIENCE MANAGEMENT SYSTEMS

In order to support compliance with this Policy and ensure a systematic, traceable, and risk-based approach, BRUC shall establish, maintain, and improve the management systems that are necessary or appropriate in light of its context, operating model, regulatory obligations, contractual commitments, and risk exposure. These management systems shall be aligned with internationally recognized standards and frameworks relating to information security, business continuity, cybersecurity, risk management, cloud service security, and other related areas.

In particular, BRUC shall structure its security model through an Information Security Management System (ISMS), aimed at establishing the framework for governance, risk management, control definition, monitoring, measurement, auditing, review, and continuous improvement of information security. Likewise, where applicable, BRUC may rely on a Business Continuity Management System (BCMS), as well as on other complementary systems, frameworks, or methodologies that strengthen operational resilience, asset protection, the security of outsourced services, and compliance with applicable legal, regulatory, normative, and contractual requirements.

The implementation and maintenance of these management systems do not replace compliance with this Policy or the regulations implementing it, but rather constitute a structured mechanism for their execution, monitoring, evaluation, and continuous improvement.

Each management system shall, where applicable, have a defined scope, assigned responsibilities, documented processes, indicators, review mechanisms, risk management procedures, deviation treatment processes, and sufficient evidence to demonstrate its effective operation.

13. NON-COMPLIANCE

Failure to comply with this Policy or with the regulations implementing it may result in the adoption of corrective, disciplinary, contractual, organizational, or legal measures, in accordance with BRUC's internal regulations, applicable legislation, and the corresponding contractual obligations.

The response to non-compliance shall be proportionate to the nature of the facts, their severity, intentionality, recurrence, actual or potential impact, the criticality of the affected assets, and the residual risk generated for BRUC, its stakeholders, or its legal and regulatory obligations.

Without prejudice to any applicable measures, any significant non-compliance shall be analyzed in order to identify its causes, assess its impact, define the necessary corrective actions, and prevent its recurrence.

14. ETHICS CHANNEL

If there are reasonable grounds to suspect a breach of this Policy or if any act contrary to the law or business ethics that could affect BRUC has occurred, such suspicion must be reported to BRUC through the established channels.

To this end, the Group has set up the Ethics Channel, an internal information system through which BRUC Professionals, directors, suppliers or any third party must report possible criminal or administrative offences or any illegal or unethical conduct, breaches of this Code or applicable legislation committed in the context of the Group's activity.

Access to the Ethics Channel can be made via the following route: https://brucenergy.integrityline.com/frontpage.

Communications made through the Ethics Channel will be handled in accordance with BRUC's Ethics Channel Policy and the safeguards recognised therein. BRUC accepts anonymous communications.

All communications will be treated in the strictest confidence, and no retaliation will be taken against the informant for making the report, unless it was made in bad faith, in which case BRUC may take any measures it deems appropriate.

15. APPROVAL AND ENTRY INTO FORCE

This Policy was approved by the Board of Directors of BRUC on 23 June 2026 and shall enter into force on the day following its approval. It is available to all Professionals and directors, as well as to all the Group's stakeholders, through its corporate website (https://brucenergy.com/).

This GISP shall be reviewed at least annually and additionally whenever significant changes occur in the risk context, business strategy, the Group, technological architecture, applicable regulations, contractual obligations, or the threat landscape that may affect its adequacy or effectiveness.