QuintasGroup
MANAGING POWER

Information Security Policy

Quintas Group Policy

Table of contents

Information Security Policy

1. Purpose

The purpose of this information security policy (hereinafter, the "Policy") is to provide a structured and clear framework of reference that sets the guidelines for our organisation in the management and protection of the information it handles, in accordance with the applicable regulations and with the ethical values of Quintas Group (also, "Quintas") as defined in its Code of Ethics[1] .

Quintas considers the information it handles as one of its most critical assets, therefore, it shall guarantee the protection of the information, regardless of the way in which it is transmitted, shared, projected or stored (hereinafter referred to as the "Information"). This protection shall cover both the information present within Quintas and the information shared with third parties.

In this context, Information Security is defined as the protection of (i) Quintas proprietary information, whether held in internal or third-party systems; and (ii) information belonging to third parties that is hosted on Quintas systems.

Finally, for the purposes of this Policy, an information system is understood to be the set of technologies, processes, business applications and software available to people at Quintas ("Information System").

2. Scope

This Policy shall apply to the entire Quintas Group and shall be binding on all its employees and external collaborators, regardless of their position and function.

The applicability of the Policy may be extended, in whole or in part, to any individual and/or legal entity associated with Quintas Group through a relationship other than an employment relationship, provided that it is feasible given the characteristics of such relationship and is beneficial to achieving the objectives established by the same.

This Information Security Policy must be adopted and applied by each of the companies of Quintas Group. Consequently, each of the companies that make up Quintas Group must use the Security Policy as a minimum requirement and adapt it to their local conditions and legislation.

Likewise, the application of this Policy is complementary to other mandatory internal rules, such as the Privacy Policy.

[1] https://www.quintasenergy.com/

The Policy shall be made available on Quintas' website[2] and on Quintas' server[3] , so that it is accessible to all interested parties.

3. Objectives

The objective of the Policy is to set guidelines for all information systems operated by the company to be secure in accordance with the following parameters:

1. Ensure the necessary degree of confidentiality for each type of information by protecting the information and restricting access only to authorized persons.

2. Maintain the integrity of the Information, avoiding alterations with respect to the time at which it was generated by the owners or persons responsible for it.

3. To ensure the availability of the Information, on all media and whenever necessary, ensuring business continuity and compliance with all obligations that may be demanded of Quintas.

4. General Principles

The objectives listed above shall be formalised in accordance with the following general principles:

- Management commitment and leadership: To ensure effective information security, it is essential to have the commitment and support of all levels of management at Quintas.

- Categorisation of information: The classification of information shall be carried out considering its value, importance and relevance to the business. This will enable protection measures to be adapted in accordance with the classification level assigned to each information asset. Likewise, the classification of information assets shall be carried out taking into account legal and operational requirements, as well as established good practices and standards.

- Use of information systems: Use of the systems shall be restricted to legitimate and exclusively professional purposes, aimed at the execution of job-related responsibilities. Consequently, personal use of these resources is prohibited, and any activity for illegal purposes is strictly forbidden.

[2] https://www.quintasenergy.com/
[3] Repository of corporate policies only accessible by Quintas employees. Z:\00.GENERAL. POLICIES

- Segregation of Duties: Risk situations resulting from a lack of segregation of duties and exclusive reliance on one person for tasks critical to the operation of the business shall be avoided. In this context, procedures shall be implemented to supervise the assignment of permissions in the Information Systems, ensuring that users access only the resources and information essential for the fulfilment of their responsibilities.

- Risk management: The integration of risk analysis and risk management shall constitute an integral part of the information security process, minimising risks to acceptable levels. The reduction of these levels shall be achieved through the implementation of security measures, balancing the nature of the data and their processing, the impact and likelihood of the risks to which they are exposed, and the effectiveness and associated cost of such security measures.

- Operational Continuity: A *Business Continuity Plan* will be implemented to ensure the recovery of critical information for the Quintas group in disaster situations, with the aim of reducing downtime to acceptable levels.

- Continuous Improvement: Security measures will be periodically reviewed and updated in order to adapt their effectiveness to the constant evolution of risks and protection systems. The treatment of information security will be supervised, reviewed and audited by qualified professionals in the area.

- Training and Awareness: To be aware of information security risks, as well as to know and apply the necessary practices to protect information.

5. Controls

It is the responsibility of all Quintas management staff to ensure that individuals adhere to this policy. Quintas' internal control staff will review the company's performance in implementing this policy.

6. Disciplinary actions

Violation of the rules, policies and procedures presented in this document by an employee will result in disciplinary action, ranging from warnings or reprimands to dismissal. Please refer to the QE Employee Handbook, section "DISCIPLINARY PROCEDURES".

7. Communication and Revision of the policy

This policy is subject of appropriate communication, training and awareness-raising activities to ensure that it is properly understood and put into practice.

This policy is reviewed periodically. The last review was carried out on 05 December 2023, reaffirming our commitment to information security.

Approved by:

Declan O'Halloran

CEO

Quintas Energy, S.A.

Version Control

Date	Version	Author/s	Notes
05/12/2023	01	Compliance	New policy created, separating previous policy from standards and procedures.

QuintasGroup
MANAGING POWER

SEVILLE LONDON MIAMI ROME BRISBANE CORK