QuintasGroup
MANAGING POWER

Information Security Policy

Quintas Group Policy

Doc. QG-POL-0009.EN

Table of Contents

Version Control

Date	Version	Author/s	Notes
05/12/2023	01	Julia Obermoller	New policy created, separating previous policies from standards and procedures
27/03/2025	02	Francisco Domínguez	Compliance with requirements of ISO 27001:2023 Standard, including climate change.

Introduction

"Information security is the preservation of confidentiality, integrity and availability of information by applying a risk management process."

The purpose of this Information Security Policy is to demonstrate Quintas Energy's commitment to safeguarding information assets and ensuring the resilience of its operations in the face of evolving threats, in alignment with ISO/IEC 27001:2023.

This policy applies to all internal and external stakeholders involved in information handling at Quintas Energy. Copies of this policy will be readily available to relevant stakeholders.

This policy will be reviewed annually or following significant internal or external changes.

Quintas Energy is committed to:

1. Operating an ISO 27001:2023-Compliant Information Security Management System (ISMS)
   Implementing an ISMS that:
   - Complies with ISO/IEC 27001:2023 requirements.
   - Supports the achievement of strategic objectives.
   - Is embedded across all business units and levels of the organisation.
   - Is documented, maintained and continuously improved.
   - Assesses whether climate change is a relevant issue in the context of the organisation, and integrates this consideration into the ISMS.

2. Governance, Risk, and Compliance
   Maintaining a documented framework to identify, assess, treat, and monitor information security risks, incorporating:
   - The Statement of Applicability (SoA) for selecting, justifying, and monitoring applicable controls.
   - Compliance with legal, regulatory and contractual requirements.
   - Inclusion of third-party and supply chain information security governance.
   - Monitoring supplier performance and compliance with IMS requirements.
   - Note: Relevant interested parties can have requirements related to climate change. Quintas Energy includes these within its stakeholder analysis.

3. Information Security Objectives and Monitoring
   Defining measurable information security objectives aligned with business goals, reviewed annually and supported by:
   - Regular performance evaluations.
   - Internal audits and continuous improvement.
   - Management reviews as per ISO/IEC 27001 Clause 9.3.

4. Asset Protection and Classification
   Ensuring that all information assets are:
   - Inventoried and classified according to their sensitivity (confidentiality, integrity, availability).
   - Labelled and handled according to documented procedures.

- Accessed only by authorised personnel on a need-to-know basis.

5. Training and Awareness

   Providing periodic training and awareness programmes to:
   - Promote a strong security culture.
   - Ensure all staff understand their responsibilities in safeguarding information.
   - Address new and emerging threats such as social engineering fraud (SEF), phishing, ransomware, etc.

6. Supplier and Outsourced Services Security

   Applying security controls throughout the supplier lifecycle:
   - Enforcing pre-qualification and due diligence based on risk.
   - Requiring contractual commitments for information security.
   - Monitoring supplier performance and compliance with ISMS requirements.

7. Business Continuity and Incident Response

   Maintaining robust plans to:
   - Ensure continuity of critical operations during disruptions.
   - Respond to, manage, and learn from information security incidents.
   - Test and improve continuity and incident response arrangements regularly.

8. Continuous Improvement and Threat Adaptation

   Embracing continuous improvement by:
   - Monitoring new and emerging threats (e.g., cyber risks, climate-driven vulnerabilities).
   - Applying a risk-based, data-driven approach to system improvements.
   - Ensuring lessons learned are incorporated into system updates and awareness campaigns.

9. Information Governance and Documentation Control

   Ensuring documented policies, procedures and records are:
   - Controlled, reviewed, and approved according to the QG Document Control Procedure.
   - Accessible to relevant internal and external stakeholders, where appropriate.

Declan O´Halloran	Aida Durnes	Rafael Hueso	Francisco Domínguez
Managing Director	Chief Operating Officer	Chief Information Officer	Global Head of HSE

QuintasGroup
MANAGING POWER

SEVILLE LONDON MIAMI ROME BRISBANE CORK