Information Security Policy

Security Policy

Introduction

This Information Security Policy is established to protect the **confidentiality, integrity, and availability** of the information assets of Qalea. It complies with the ISO/IEC 27001:2022 standards and applies to all employees, contractors, and third-party users who access or use the information assets of Qalea.

Purpose

The purpose of this policy is to ensure the protection of information assets from all threats, whether internal or external, deliberate or accidental. It aims to ensure compliance with all applicable laws, regulations, and contractual obligations.

The policy establishes a framework for setting, reviewing, and achieving information security objectives and defines the responsibilities of employees, contractors, and third-party users in protecting the information assets of Qalea.

Additionally, the policy aims to promote awareness, educate employees, and guide decision-making processes related to information security within the organization.

Scope

Qalea Cybersecurity, a company dedicated to cybersecurity solutions, has decided to introduce a Information Security Management System , to improve the services provided to its clients.

This policy applies to all information assets owned, leased, handled or otherwise controlled by Qalea, including information stored on physical or electronic media, information transmitted over networks or through any communication channels, and information processed or handled by employees, contractors, or third-party users.

Objectives

The primary objectives of this policy are to protect the **confidentiality** of information to prevent unauthorized disclosure, ensure the **integrity** of information to prevent unauthorized modification, and ensure the **availability** of information to authorized users when needed.

Additionally, the policy seeks to ensure compliance with **applicable laws, regulations, and contractual obligations** such as the General Data Protection Regulation (GDPR), the Spanish Data Protection Act (LOPDGDD),Law 10/2021 on Remote Work, etc.. while **continuously improving** the information security management system (ISMS).

Security Organization & Responsibilities

Qalea Management is responsible for providing leadership and commitment to information security. They ensure that adequate resources are available to implement and maintain the information security management system and review and approve information security policies and procedures.

The Information Security Management System Responsible (ISMS Responsible) is responsible for developing, implementing, and maintaining the information security management system. This includes conducting risk assessments, implementing appropriate controls, and reporting on the effectiveness of the information security management system to senior management.

Employees, contractors, and third-party users are responsible for complying with this policy and all related information security procedures. They must report any suspected information security

incidents or vulnerabilities to the ISMS Responsible and participate in information security training and awareness programs.

Security Measures

Aligned with our commitment to safeguarding information assets and maintaining the integrity of our operations, we have established a comprehensive set of security measures. These measures encompass a range of strategies and technologies aimed at protecting our systems, data, and resources from potential threats, ensuring the confidentiality, integrity, and availability of information critical to our business.

- **Human Resources:** Human resource security measures are implemented to ensure that employees, contractors, and third-party users are aware of their responsibilities and are equipped to safeguard information assets.
- **Asset Management:** Asset management measures are implemented to ensure that all information assets are properly identified, classified, and secured throughout their lifecycle. This includes maintaining an accurate inventory of assets, assigning ownership, and defining usage guidelines. Regular audits and reviews are conducted to ensure assets are adequately protected.
- **Access Control:** Access to information assets is limited to authorized users only. Strong authentication and authorization mechanisms are implemented, and access rights are periodically reviewed to ensure they remain appropriate.
- **Network Security:** Measures are implemented to secure the company's network infrastructure against unauthorized access, breaches, and other security threats. This includes firewalls, intrusion detection systems, and regular network monitoring.
- **Operations Security:** Operations security measures are enacted to preserve the integrity of operational processes and guarantee the secure execution of daily activities. This includes implementing robust monitoring systems and logging mechanisms to swiftly identify and respond to suspicious activities.
- **Configuration Management:** A configuration management procedure is implemented to ensure that all configurations of information systems and related assets are systematically managed, documented, and monitored throughout their lifecycle. This process supports the organization's information security objectives by maintaining the integrity and consistency of configurations.
- **Secure Development:** Security practices are integrated into the software development lifecycle to ensure that applications are designed, developed, and maintained securely. This includes code reviews, vulnerability assessments, and regular security testing.

- **Change Management:** A procedure is established to control and document changes to information systems and infrastructure. This ensures that changes are reviewed, approved, and implemented in a controlled manner, minimizing the risk of security incidents and operational disruptions.
- **Risk Management:** Regular risk assessments are conducted to identify and evaluate risks to information assets. Appropriate controls are implemented to mitigate identified risks, and the effectiveness of these risk management activities is continuously monitored and reviewed.
- **Data Management:** Information is classified based on its sensitivity and criticality. Appropriate handling procedures are defined for each classification level to ensure the protection of information throughout its lifecycle.
- **Incident Management:** An incident management process is established and maintained to detect, respond to, and recover from information security incidents. All security incidents must be reported promptly to the designated incident response team. Incidents are investigated to determine the root cause and to prevent recurrence.
- **Business Continuity:** Plans are established and maintained to ensure the continuation of critical business functions in the event of a disruption. Regular tests and updates to these plans are conducted to ensure their effectiveness.
- **Third-Party Management:** Security requirements are defined and enforced for third-party vendors and partners. Regular assessments and reviews are conducted to ensure that third parties comply with the company's information security standards.
- **Compliance:** Compliance with all relevant laws, regulations, and contractual obligations related to information security is ensured. Regular audits and reviews are conducted to verify compliance with this policy and the information security management system.
- **Awareness and Communication:** Regular information security training is provided to all employees, contractors, and third-party users. Awareness of information security policies, procedures, and best practices is promoted throughout the organization.

Security Improvement

Qalea is committed to the principle of **continuous improvement** in its information security management practices. Regular assessments and reviews are conducted to identify areas for enhancement in the ISMS. Feedback from audits, incident reports, and employee suggestions are systematically evaluated to implement improvements. Metrics and performance indicators are monitored to measure the effectiveness of information security controls and to identify opportunities for refinement. Continuous improvement efforts ensure that the ISMS remains effective, responsive to emerging threats, and aligned with the strategic objectives of Qalea.

Management Team,

Qalea Cybersecurity

28th February 2025