Information Security Policy

2023

VASS

complex made simple

Index

1. Object

The Management of **VASS Consultoría de Sistemas S.L.** (hereinafter VASS), within the strategy defined for the development of the business, considers information security a fundamental aspect to ensure the achievement of business objectives and compliance with current legislation. Therefore, it is committed to maintaining an adequate level of security, aligned with the business, in the processes associated with the services provided by the organization, in order to offer its internal and external customers the best guarantees in terms of the quality of such services.

2. Security Policy Objectives

VASS provider of digital solutions whose mission is to help clients transform opportunities into business.

For the fulfillment of its Mission, the provision of Services and the achievement of its objectives, **VASS** depends on ICT systems. These systems must be managed with diligence, taking appropriate measures to protect them against accidental or deliberate damage that may affect the confidentiality, availability, integrity, authenticity and traceability of the information processed or services provided.

With the implementation of an ISMS under the UNE ISO/IEC 27001 Standard integrated, the security of the services, as well as of the information and data included in these services and necessary for their correct and adequate provision is strengthened, due to the close relationship between both and the additional elements that significantly improve the security management necessary for **VASS**, as part of the satisfactory fulfillment of its mission.

The objective of information security is to guarantee the quality of information and the continuous provision of services, acting preventively, monitoring daily activity and reacting promptly to incidents.

Within this context, the objectives of this Information Security Management System Policy are:

- Guarantee the confidentiality, availability, integrity, authenticity and traceability of information.
- Manage existing security risk to the thresholds established by management, based on service delivery to customers.
- Implement an SGSI to manage and protect the information and services provided by the company.
- Implement a set of appropriate security measures or controls, determined by the UNE ISO/IEC 27001 Standard, as well as any additional controls identified, as part of the ISMS to ensure protection against threats that may affect the authenticity, traceability, confidentiality, integrity, availability, intended use and value of information and services. through threat and risk assessment.
- Appoint an SGSI manager, in charge of managing the system and ensuring its development, maintenance and improvement.
- Appoint a Security Manager and ensure that he/she has the necessary resources to carry out the necessary information security controls.
- Establish a methodology for review, audit and continuous improvement of the SGSI, following a PDCA cycle that guarantees the continuous maintenance of the desired security levels.
- Periodically establish a set of information security management objectives and indicators that allow management to adequately monitor the level of security and compliance with the objectives.
- Ensure that the organization's in-scope personnel have sufficient knowledge of information security policies and controls.
- Ensure that information security incidents are correctly identified, managed and resolved.
- Comply with all applicable legal, statutory, regulatory requirements and contractual obligations.
- Ensure the continuity of the business processes included in the scope.

3. SGSI

VASS Management is committed to allocate the necessary resources and means to establish, implement, maintain and improve the ISMS and the necessary security controls, maintaining an appropriate balance between cost and benefit, as well as to demonstrate leadership and commitment to it.

3.1. Establishment, deployment and improvement of the SGSI

The establishment and deployment of the SGSI of **VASS** will start from the Risk Analysis, which will determine the level of information security risk in which **VASS** finds itself and identify the security controls necessary to address the risk and bring it to an acceptable level, as well as opportunities for improvement, considering internal and external issues and stakeholder requirements.

Security controls shall be implemented, maintained and continually improved, and made available as documented information, through procedures, regulations, technical instructions, and any other documentation deemed necessary, reviewed and approved by the Information Security Committee.

The documented information of the security controls shall be communicated to the personnel working in **VASS** (employees and suppliers), who shall have the obligation to apply it in the performance of their work activities, thus committing themselves to comply with the requirements of the SGSI**.**

3.2. Evaluation

Audits will be carried out periodically to review and verify compliance of the ISMS with the requirements of ISO/IEC 27001 within the regulatory framework of the ENS, so that, if necessary, the personnel affected by the scope must collaborate in these audits, as well as in the implementation of the corrective actions derived for continuous improvement. Qualification criteria will be defined for the persons performing such audits.

4. Staff Obligations

Managers of **VASS** departments included within the scope of this policy shall be responsible for ensuring compliance with these policies within their departments.

All **VASS** employees have the obligation to know this Information Security Policy and the Security Regulations that develop it, which are mandatory within the scope identified, being the responsibility of the Security Committee to provide the necessary means to ensure that the information reaches those affected.

All contracted personnel must receive and sign a commitment to comply with the information security policy and security regulations, and must receive training or awareness training related to information security, depending on their position.

Contact Information

Av de Europa, 1, edificio B. 28108 Alcobendas, Madrid, Spain

info@vasscompany.com

+34 91 662 3404