Information Security and Business Continuity Policy

2024

VASS

complex made simple

Index

1. Object

The Management of VASS Consultoría de Sistemas SL (hereinafter VASS), within the strategy defined for the development of the business, considers information security and business continuity as fundamental aspects to ensure the achievement of business objectives and compliance with current legislation. Therefore, it undertakes to maintain an adequate level of security and aligned to 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. Policy objectives

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

For the fulfilment of its mission, the provision of services and the achievement of its objectives, VASS depends on ICT systems. These systems must be managed diligently, taking appropriate measures to protect them against accidental or deliberate damage that could affect the confidentiality, availability, integrity, authenticity and traceability of the information processed or the services provided.

With the implementation of an Integrated Management System (hereinafter IMS) under the UNE ISO/IEC 27001 and UNE-EN-ISO 22301:2020 Standards, the security and continuity of services is strengthened, as well as the information and data included in these services and which are necessary for their correct and adequate provision, due to the close relationship between both and the additional elements that significantly improve the security management that is necessary for VASS, as part of the satisfactory fulfilment of its mission.

The objective of information security and business continuity is to ensure the quality of information and the continued provision of services by acting proactively, monitoring daily activity and reacting promptly to incidents.

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

- Guarantee the confidentiality, availability, integrity, authenticity and traceability of information.
- Manage existing security risk to the thresholds set by management, based on the provision of service to customers.
- Implement an MIS to manage and protect the information and services provided by the company.
- Implement a set of appropriate security measures or controls, as determined by the UNE ISO/IEC 27001 Standard, as well as any additional controls identified, as part of the MIS 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 IMS manager, responsible for managing the system and ensuring its development, maintenance and improvement.
- Appoint a Security Officer 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 IMS, following a PDCA cycle to ensure that the desired safety levels are continuously maintained.

- Periodically establish a set of objectives and indicators for information security and business continuity management that allow management to adequately monitor the level of security and compliance with the objectives.
- Ensure that in-scope personnel of the organisation have sufficient knowledge of information security and business continuity policies and controls.
- Ensure that information security incidents are correctly identified, managed and resolved.
- Comply with all applicable legal, regulatory, statutory requirements and contractual obligations.
- Ensure the continuity of the business processes included in the scope.

3. GIS

VASS management is committed to allocate the necessary resources and means to establish, implement, maintain and improve the MIS 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 GIS

The establishment and deployment of the VASS MIS will start from the Risk Analysis, which will determine the level of information security and business continuity 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, policies, technical instructions, and any other documentation deemed necessary, reviewed and approved by the Information Security and Business Continuity Committee.

Documented information on security controls must be communicated to VASS personnel (employees and suppliers), who are obliged to apply it in the performance of their work activities, thereby committing themselves to compliance with the requirements of the IMS.

3.2. Evaluation

Audits shall be carried out periodically to review and verify the compliance of the MIS with the requirements of ISO/IEC 27001, whereby, if necessary, the personnel affected by the scope shall collaborate in these audits, as well as in the implementation of corrective actions for continuous improvement. Qualification criteria shall 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 are obliged to know this Information Security and Business Continuity Policy and the Security Regulations that develop it, which are mandatory within the identified scope, being the responsibility of the Security Committee to provide the necessary means for the information to reach those affected.

All recruited personnel shall receive and sign a commitment to comply with the information security and business continuity policy and security regulations, and shall receive information security and business continuity training or awareness training, depending on their position.

Contact Information

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

info@vasscompany.com

+34 91 662 3404