INFORMATION SECURITY POLICY

MOTIVATION

Companies' lack of control over how data and information are generated, where they are stored, and to whom they are transmitted poses the risk of security and regulatory compliance incidents that can negatively impact the business itself. Information security is a primary asset for a company, and implementing effective measures can be a strategy that ultimately turns into a competitive advantage.
For this reason, GIMASI DEUTSCHALAND GMBH, an information technology services company, has always been at the forefront of data protection issues. A key measure in this regard has been the implementation of an Information Security Management System, a set of organizational, technical, and procedural processes based on best practices and reference standards, also in compliance with the directives and the international standard ISO/IEC 27001:2022.

GOALS

The objective of GIMASI's Information Security Management System is to ensure an adequate level of protection and security for the circulation of information within the organization in order to best carry out the design, development, and delivery of company services.
Without risk identification, assessment, and analysis procedures, the security risks to which company services and procedures are exposed on a daily basis can jeopardize their proper functioning, with significant economic consequences.
The set of organizational, technical, and procedural measures established by GIMASI's Information Security Management System satisfies the following basic security requirements:

- Confidentiality: Access to information is permitted only to those with privileges.
- Integrity: information management (and therefore also its modification) is subject to precise constraints set by corporate governance
- Availability: rights holders can freely access information as soon as they feel the need to use it within operational processes and retrieval occurs quickly and intuitively.

GIMASI aims to position itself in the field of information security as:

- A reliable and competent supplier to best preserve the company's image
- A hub where corporate information assets are stored, safeguarded and protected
- A facilitator of business process continuity
- A tool that complies with the provisions of current and binding legislation, with the consequent growth of corporate skills in safety matters

Gimasi Deutschland GmbH
Lindwurmstr 97a, 80337 München
DE319590118
+49 89 20002118-0
support@gimasi.de

POLICY CONTENT

Any information required for internal operations, from product/service data to its configuration, must be protected throughout its lifecycle, from creation to use to disposal. The Information Security Management System fits into this process, enabling secure, accurate, and reliable information management and timely recovery.

In accordance with the current ISO/IEC 27001:2022 regulation Among the preventative measures required by the Information Security Management System is the mandatory assessment of security risks and their potential impact on the company, which must be performed periodically by the Information Security Manager.
This assessment assesses whether the aforementioned security requirements are being met, analyzes the critical factors that led to incidents, and places them within a broader context of strategic, business, and technological changes already implemented or to be implemented.

This analysis aims to assess the risk associated with each asset to be protected against the identified threats. The procedure adopted by the Information Security Manager in performing this assessment is shared with Management, which must approve the document detailing the methodology to be applied. Furthermore, Management also contributes to defining the parameters that define the risk level. Once the Manager has completed his or her analysis, the results are jointly evaluated with Management, which determines whether the risk threshold is acceptable or not based on the previously established metrics. Finally, risk mitigation measures, if deemed necessary, are defined, along with the actions to be taken to improve system security, based on company priorities and budget, and the need to comply with applicable regulations.
All of this will be carefully considered, taking into account the value of the information to be protected and the presence of events that could significantly impact system security.

RESPONSIBILITY

Responsibilities are distributed as follows:

- the STAFF who are responsible for compliance with the agreed privacy policy and who must report any anomalies to the manager, if they find them
- the INFORMATION SECURITY COMMITTEE, which meets at least twice a year. Its members include Management and the Information Security Manager, but the involvement of company personnel with the technical expertise necessary to assess specific aspects is not excluded. As already mentioned, Management is responsible for establishing priorities and promoting security initiatives, ensuring compliance with company strategies and project budgets.
- the INFORMATION SECURITY MANAGER: his or her responsibility is to draft and design the Information Security Management System.

Specifically, the risk analysis and management team identifies the most appropriate criteria and methodologies, and oversees the necessary regulations, including those regarding document classification, so that the company can operate smoothly and securely. The assessment also involves the Manager proposing appropriate security measures and reviewing any incidents that have occurred, which are then addressed with the appropriate countermeasures.
The team is also committed to promoting a culture of information security and offering training programs for staff.

- EXTERNAL PARTIES who come into contact with GIMASI must respect the indicated security principles and sign, unless clearly stated in the contract, a "confidentiality agreement" upon assignment.

APPLICABILITY

This privacy policy applies to all internal and external company bodies and is valid for all GIMASI personnel. It also applies to any external party who gains access to information handled within the company, requiring prior agreement to ensure external communication complies with applicable rules and regulations.

REVIEW

GIMASI will ensure the periodic review of the effectiveness and efficiency of the Information Security Governance System. Where necessary and appropriate to the context and business objectives, it will adopt the necessary measures to improve security policies and ensure their correct implementation to ensure the continuous and secure execution of all company processes.

Monaco, 11/11/2024

Gimasi Deutschland GmbH

Gimasi Deutschland GmbH
Lindwurmstr 97a, 80337 München
DE319590118
+49 89 20002118-0
support@gimasi.de