LEVIAhub
SUPPLY CHAIN MASTER

Information Security Management System Policy

Information Security Management System Policy

The Management and the staff of LEVIAHUB S.p.A. place information security at the foundation of their activities, whose primary objective is the protection of the company's information assets, in order to minimize the risk of damage caused by deliberate or accidental security incidents from within, from outside, or from potential threats to the company itself as well as to the company's customers who use the products created by LEVIAHUB S.p.A. Responsibility for applying this Policy and managing the system concerns the entire Company Organization, from Management down to every individual employee, according to their respective roles and competencies.

To achieve this primary objective, LEVIAHUB S.p.A. pursues the following goals:

- ensure compliance with applicable mandatory regulations;
- identify, through appropriate risk analyses, the value of information assets in order to understand the vulnerabilities and possible threats present in the company that may expose it to the risk of failing to achieve objectives;
- manage risk at an acceptable level through the design, implementation, and maintenance of appropriate information security countermeasures, in order to ensure the quality of the products and services provided;
- protect the confidentiality of information by ensuring that information is accessible only to those who are authorized, and by classifying information that requires a certain degree of confidentiality;
- protect the integrity of information by safeguarding, as far as possible, its accuracy and completeness as well as the methods used to process it;
- protect the availability of information by ensuring that authorized users can effectively access the information and assets necessary for their work whenever they require it;
- act promptly and effectively in response to needs arising during work activities;
- draw up emergency plans, contingency plans and, where necessary, business continuity plans, keeping them as up to date and monitored as possible.
- periodically review the Policy, the Objectives, and the implementation of the Management System in order to achieve continuous improvement of the level of information security in the company.

In applying its Management System, LEVIAHUB S.p.A. applies the mandatory rules concerning the protection of personal data in compliance with EU Regulation 679/2016 (GDPR), Directive 2555/2025 (the so-called NIS2 Directive), and any related laws and Regulations. For this reason, data is processed by LEVIAHUB S.p.A. in a lawful, fair, and transparent manner, solely for the purposes deemed necessary and solely for the necessary operations (principle of minimization). LEVIAHUB S.p.A. is also committed to the maintenance of accurate data, updating it when necessary and storing it only for the time deemed strictly necessary for carrying out company activities. LEVIAHUB S.p.A. guarantees data subjects access to their personal data within the limits established by Law, as well as the right to erasure and the right to be

forgotten in specific identified cases. It is committed to protecting its data with appropriate technical measures and with the support of the procedures provided for by the Management Systems.
No less important for the improvement, effectiveness, and efficiency of the organization is an approach based on the prevention of problems rather than on after-the-fact control and the related correction, so as to significantly reduce the probability of incidents or other non-conformities occurring. Human resources at all levels represent the fundamental element for achieving the planned objectives: they are made aware of the company's information security objectives by promoting the implementation of specific training programs and by valuing the results achieved.
All company personnel and suppliers who are in any way involved in the scope of the Management System are responsible for implementing this policy, with the support of Management, which has approved the policy itself.
The Company aims to manage Information Security Events, to prevent – as far as possible – Information Security incidents and, where this is not feasible, at least to manage all information security breaches and possible weaknesses, which must be reported to the appropriate parties and investigated, in compliance with mandatory and regulatory provisions.
The Information Security Management System is intended to provide consistent results to Management in order to set appropriate assessments and its own objectives for the Management System itself in a coherent and considered manner, so as to make appropriate decisions taking into account the organizational context, the risks, and the available opportunities.
This policy is formulated and reviewed by Company Management. All personnel, based on their own knowledge, have the responsibility to report to the System Manager any weakness identified in the company systems.
This policy is reviewed regularly in order to identify any changes that affect it and to ensure that it remains suitable for the organization's purposes and the expectations of stakeholders.

Company Management