Information Security Policy

The information security policy aims to protect the organization's information resources from threats (internal, external, intentional, accidental threats) that can compromise the confidentiality, integrity and availability of information.

In particular the organization undertakes the following activities:

- The information is accessible exclusively to authorized persons, both internal and external to the company,
- guaranteeing service levels and complexity compatible with the functional requirements of the systems involved;
- Whatever the format of the information processed, its availability, integrity and confidentiality is guaranteed compliance with applicable legislative requirements;
- Constant monitoring of changes in assets and technology is carried out in order to identify new vulnerabilities promptly;
- Constant updating is carried out on sites specialized in security issues and prompt forums identification of new types of threats;
- Particular attention is paid to changes in regulatory and contractual requirements and related priorities relation to new application developments;
- Operational continuity is guaranteed through targeted interventions, both organizational and technological, and that such interventions are defined, constantly updated and periodically verified;
- All staff are trained on safety and are informed of the mandatory nature of company policies merit and who is also made aware of the consequences resulting from the violation of company policies;
- Periodic assessments of the effectiveness of the ISMS and staff training are carried out through simulations within the scope of application (penetration/intrusion tests on logical-physical security, policy knowledge tests and simulations of violations thereof);
- Metrics are introduced for evaluating system performance;
- Duties relating to critical activities are separated (for example development and testing with production);
- Risks at source are reduced as much as possible;
- Any security breach, real or perceived, is reported and investigated;
- Security incidents are promptly identified and managed and the competent authorities are activated for those that have an impact on violated legal requirements;
- The use of unauthorized software is avoided;
- Periodic REVIEWS of the ISMS are carried out in relation to:
  - verification of the currency and effectiveness of the controls applied for the threats and vulnerabilities identified in the plan
  - risk treatment;
  - impact of the controls implemented on management effectiveness;
  - or changes brought about by technology (new or modified vulnerabilities, risk reduction for new
  - knowledge acquired based on technological progress);
  - changes made to the configuration of systems under ISMS;
  - periodic reassessment of the risk and in particular before and after any preventive action.

The organization also:
Defines the risk assessment methodology based on the ISO/IEC 27005 guidelines.
Identify the objectives and related monitoring parameters for managing system performance.

Responsibility for the establishment and management of the SGSI is assigned to the Information Security Manager

Como, 03.11.2023

CEO

dı