

INFORMATION SECURITY POLICY

The purpose of the information security policy is to protect the resources included in the ISMS (Information Security Management System) from threats (internal, external, deliberate, accidental) that may compromise them, primarily guaranteeing the Confidentiality, Integrity and Availability of information.

In particular, for all systems under ISMS, the organisation shall ensure that:

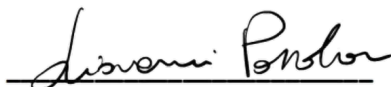
- Information is accessible only to authorised persons, both internal and external to the company, guaranteeing levels of service and complexity compatible with the functional requirements of the systems concerned;
 - Whatever the format of the information processed, its availability, integrity and confidentiality are guaranteed in compliance with the applicable legislative requirements;
 - Constant monitoring of changing assets and technology is carried out in order to promptly identify new vulnerabilities; and Special attention is paid to changes in regulatory and contractual requirements and priorities in relation to new application developments;
 - Business continuity is guaranteed through targeted organisational and technological interventions, and that these interventions are defined, constantly updated and periodically verified;
 - All personnel are trained on security, that they are informed of the mandatory nature of company policies in this regard and that they are also made aware of the consequences of violating company policies;
 - Periodic evaluations of the effectiveness of the ISMS and staff training are carried out through simulations in the field of application (logical/physical security penetration/intrusion tests, policy knowledge tests and simulations of policy violations);
 - Metrics for evaluating system performance are introduced;
 - Tasks related to critical activities are separated (e.g. development and testing with production);
 - Risks are reduced as much as possible at source;
 - Any actual or suspected security breaches are reported and investigated;
 - Security incidents are promptly identified and handled, and the competent authorities are activated for those that impact on violated legal requirements;
 - The use of unauthorised software is prevented;
- Periodic reviews of the ISMS are carried out with regard to:
- verification of the relevance and effectiveness of the controls implemented for the threats and vulnerabilities identified in the risk treatment plan;
 - impact of implemented controls on management effectiveness;
 - changes brought about by technology (new or modified vulnerabilities, risk reduction due to new knowledge gained from technological progress);
 - changes made to the configuration of the systems under the ISMS;
 - periodic reassessment of the risk and in particular upstream and downstream of any preventive action.

The risk assessment methodology based on the guidelines of ISO/IEC 27005 is also defined. To monitor the performance of the system, security objectives have been identified, which are measured by specific KPIs indicated in the document: *ISMS_110.IT.0-Security Objectives KPI*.

Responsibility for the establishment and management of the ISMS is assigned to the Information Security Officer.

Villorba, 01/06/2022

Security Manager
Giovanni Pozzobon



CEO
Giorgio De Nardi

