Cybersel
Cyber Risk Assessment and Prevention

Information Security Policy

The security policy for the resources included in the ISMS is to protect such resources from threats (internal, external, deliberate, accidental) that may compromise them, primarily ensuring the confidentiality, integrity and availability of the information.

In particular, for all systems under SGSI, the organization undertakes to ensure that:

- The information is accessible exclusively to authorised persons, both internal and external to the company, ensuring service levels and complexity compatible with the functional requirements of the systems involved;
- Whatever the format of the information processed, their availability, integrity and confidentiality must be guaranteed in compliance with applicable legislative requirements;
- Constant monitoring of asset and technology changes is carried out in order to promptly identify new vulnerabilities;
- Constant updates should be provided by authoritative sources specializing in security issues and by discussion and training groups to promptly identify new types of threats;
- Particular attention should be paid to changes in regulatory and contractual requirements and related priorities in relation to new application developments;
- Operational continuity must be guaranteed through targeted interventions, both organizational and technological, and such interventions must be defined, constantly updated and periodically verified;
- All personnel are trained in safety, are informed of the mandatory nature of company policies in this regard and are also made aware of the consequences of violating company policies;
- Periodic assessments of the effectiveness of the ISMS and staff training should be carried out through simulations within the scope of application (vulnerability assessment, penetration tests, policy knowledge tests and simulations of policy violations);
- Metrics for evaluating system performance should be introduced;
- Tasks and environments related to critical activities (e.g. development and testing from production) should be separated and following a policy of least privilege);
- Risks should be reduced as much as possible at source;
- Any actual or suspected breach of security is reported and investigated;
- Security incidents should be promptly identified and managed and the relevant authorities should be activated for those that impact violated legal requirements;
- Avoid using unauthorized software;
- Periodic reviews of the ISMS are carried out in relation to:
  - or verification of the relevance and effectiveness of the controls applied for the threats and vulnerabilities identified in the plan of risk treatment;
  - or impact of the controls implemented on management effectiveness;
  - or changes brought about by technology (new or modified vulnerabilities, risk reduction for new knowledge acquired on the basis of technological progress);
  - or changes made to the configuration of systems under SGSI;
  - or periodic reassessment of the risk and in particular upstream and downstream of any preventive action.

The risk assessment methodology based on the ISO/IEC 27005 guidelines is also defined and the objectives and related monitoring parameters for managing system performance are identified.
The objectives are described in the ISMS_Information Security Objective - KPI document.

The responsibility for establishing and managing the ISMS is assigned to the Information Security Manager.

Turin, March 20, 2025

CISO

Dr. Mauro Lisa

CEO

Walter Marmo