Information Security Policy

NUSO Italia Srl considers information security as its primary objective. To this end, it has decided to implement and maintain an Information Security Management System (ISMS), following the requirements specified in the UNI CEI EN ISO/IEC 27001 Standard, to guarantee:

1. Confidentiality - information accessible only to duly authorized individuals and/or processes;
2. Integrity - safeguard the consistency of the information from unauthorized changes;
3. Availability - ease of access to necessary information;
4. Control - assurance that data management processes and tools are secure and tested;
5. Authenticity - reliable origin of the information;
6. Privacy – guarantee of protection and control of personal data.

The Management's commitment is implemented through the definition of an appropriate organizational structure to:

- determine corporate roles and responsibilities for the development and maintenance of the ISMS;
- monitoring that the ISMS is integrated into all company processes and that procedures and controls are effectively developed;
- monitor exposure to information security threats;
- implement programs to spread information security awareness and culture.

Therefore NUSO Italia Srl general objectives are:

- guarantee the best standards, optimizing and rationalizing company processes and tools;
- guarantee the satisfaction of all the stakeholders of the ISMS in relation to the quality of information;
- guarantee the Confidentiality, Integrity and Availability of the information processed, whether for internal use or related to the products supplied and the services provided to customers;
- guarantee the reliability of the products developed through the application of techniques related to the development of “secure code”;
- guarantee the reliability and resilience of the services provided, ensuring customers and all stakeholders the level of business continuity expected through the adoption of adequate levels of infrastructure redundancy, data security, control over applications and change processes;
- identifying and assessing risks and opportunities, through the implementation of specific technological and organizational measures, the monitoring of their efficiency and the verification of the results achieved;
- monitor the effectiveness and efficiency of the processes adopted, with reference to the objectives set, with a view to continuous improvement;
- guaranteeing compliance with current legislation and regulations applicable to the company reality;
- foster the orientation and responsibility of its personnel towards the company's Management System through the implementation of personnel information and training programs.

This information security policy is spread throughout every sector and at all decision-making and operational levels. Periodically, during reviews of the information security management system, this policy is reviewed, together with the corporate objectives, and revised if necessary.

The Management