sdi
The power of automation

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Information Security Policy

POLI01PUB

In accordance with the International Standard ISO/IEC 27001, this document is classified as being of the PUBLIC USE level.

List of revisions

REV	DATE	AUTHOR	SHORT DESCRIPTION
00	04/04/2019		First issue
01	02/04/2021		
02	02/03/2022		Version for public use

Contents

1. Purpose and scope of application

This Information Security Policy has been drawn up in compliance with the requirements of the international standard ISO 27001 and represents the reference framework of the principles, guidelines and rules that must be adopted for the security of the information assets of s.d.i. s.p.a.
The principles, guidelines and rules contained herein are of a general nature, dedicated to the various aspects of information security and articulated according to the structure suggested by the international standard ISO 27001 and related "best practices". In particular:

- Standard ISO/IEC 27001 - Information security management systems;
- Standard ISO/IEC 27002 - Code of practice for information security controls;

And for the risk analysis process:

- Standard ISO/IEC 27005 - Information security risk management;
- Standard ISO/IEC 31000 - Risk management principles and guidelines;

The specific aims of this document are to:

- Establish general rules and basic principles for the proper management and protection of information and the information technology assets of the company;
- Fulfil the obligations imposed by laws on information security;
- Provide a common foundation of guidelines and rules for the development and implementation of operational procedures for information security management;
- Define general and specific roles and responsibilities for all aspects relating to the security of information and the IT assets of the company.

The Information Security Policy is addressed to s.d.i. s.p.a. employees and to all interested stakeholders (e.g. Customers, Suppliers and other third parties).
The scope of the Information Security Policy coincides with the perimeter of the Information Security Management System. This document will be reviewed at least once a year and, in any case, whenever there are significant changes to the elements that have an impact on the Information Security Management System and on the security of information in the company, in order to ensure its adequacy with respect to the context.

2. Information security roles and responsibilities

s.d.i. s.p.a., in relation to the corporate organizational structure and in accordance with the inter-functional dimensions of information security, has identified the following roles for the management of the Information Security Management System (ISMS):

- ISMS Manager (Technical Director);
- ISMS Coordinator (ICT Manager);
- ISMS Committee.

In addition to the roles and bodies mentioned above, the organization of the Information Security Management System also includes the following figures:

- Physical Security Manager (General Services Manager);
- Logical Security Manager (ICT Manager).

2.1 ISMS Committee

The ISMS Committee consists of the following permanent members:

- ISMS Manager (chairs the ISMS Committee);
- ISMS Coordinator;
- Physical Security Officer;
- Logical Security Officer,
- Quality and HSE Manager
- Any other Functions, involved if necessary, having a role in information security and/or external professionals, to support the Information Security Manager in the activities necessary for the setting up, maintenance and continuous improvement of the Information Security Management System.

The ISMS Committee is convened at least once every six months. The ISMS Committee meetings are preceded by an agenda and minutes are taken.

2.2 Separation of duties

s.d.i. s.p.a. applies the principle of separation of duties and responsibilities where appropriate, in order to reduce the risk of negligence or improper use of the systems. This principle must be implemented when appropriate, taking into account the specifics of the corporate situation, so as to reduce the possibility of a person making unauthorized changes or irregular use of corporate data and/or services.

3. Security in personnel behaviour

All employees, collaborators and Third-Parties involved are responsible for the protection of the information of the computer equipment owned by s.d.i. s.p.a. entrusted to them.
The employees, collaborators and third parties must apply the company policies, rules and procedures on the subject of information security, as far as they are concerned.
The management of s.d.i. s.p.a. also undertakes to:

- Require compliance with the policies, rules and procedures of the Information Security Management System by employees, collaborators and third parties involved;
- Promote the dissemination of the culture of information security within the company through the knowledge and adoption of this policy and all the rules of the Information Security Management System by employees, collaborators and third parties involved;
- Support the management bodies of the Information Security Management System in the phases of risk assessment and identification of appropriate solutions in their area of competence;
- Implement risk mitigation actions approved in compliance with the defined plan within respective areas of competence.

3.1 Information security skills and training

s.d.i. s.p.a. ensures the appropriate training, information and awareness of the employees, and of the collaborators where necessary, in order to guarantee the acquisition of the knowledge necessary to maintain the security of the company assets (goods and information) in the exercise of the tasks entrusted to them.
The management of s.d.i. s.p.a. undertakes to ensure:

- The appropriate level of competence of each employee in terms of information security is guaranteed, with respect to the specific nature of the tasks assigned;
- The appropriate actions to improve such skills are promoted, in agreement with the ISMS Manager.

3.2 Confidentiality agreement

All persons coming into possession of data and information of s.d.i. s.p.a. and its business are required to maintain the utmost confidentiality, as required by company rules and procedures concerning:

- Employees, by signing, at the beginning of the employment relationship, the "Confidentiality, Industrial and Intellectual Property and Assets Agreement".
- Third parties, when deemed appropriate, by signing contracts that include the "Non-Disclosure Agreement" and possibly also the "Confidentiality and Non-Competition Agreement".

Any forms of collaboration with s.d.i. s.p.a. that are not included in the above-mentioned cases must, in any case, be subject to the confidentiality rules.

3.3 Use of IT assets

The use of computer assets and systems, as well as the processing of company data and information, must be for work purposes only. Therefore, any use of s.d.i. s.p.a.'s assets, systems, data and information that is not for such purposes, may be considered as improper unless it has been explicitly authorized by the management of s.d.i. s.p.a. All employees and collaborators of s.d.i. s.p.a. are responsible for the protection of the assets and computer tools entrusted to them, in compliance with the company rules. The use of personal computers, the network, media, notebooks, mobile devices, electronic mail and the Internet are specifically regulated.

3.4 Teleworking and Smartworking

It is possible to connect to the company network and work remotely. Access from locations other than the company headquarters is protected by a secure connection (e.g. VPN).

3.5 Clear desk

In order to ensure the security of corporate information, all employees and collaborators of s.d.i. s.p.a. adopt a "clear desk" mode to reduce the risk of unauthorized access:

- To company data contained on their PC (or other devices), through the application of a timed screen saver equipped with an automatic lock with password request for access;
- To documents classified as "reserved" or "confidential" in one's office, through the use of drawers and cabinets with keys.

Similar attention is paid to the use of common areas (e.g. meeting rooms) and shared devices (e.g. printers, photocopiers).

4. Asset management and protection

In order to guarantee the appropriate level of information protection, all the company's information assets are catalogued and managed by an asset management tool.
Each asset (IT or production) is inventoried and assigned to a corporate department.
The Department Manager defines the appropriate security measures for the protection of the assets under his responsibility. The assignee is required to apply the security measures defined by the Department Manager.

4.1 Classification and protection of information

s.d.i. s.p.a. adopts the classification of information, with particular reference to electronic and paper documents present in the company, on the basis of their criticality in terms of confidentiality, integrity and availability.
The processing of information must be consistent with the rules defined in this Information Security Policy.
The classification of all pages of internally produced documents must be carried out by the author by affixing the relevant classification level label, in particular:

- INTERNAL USE
- Confidential;
- Highly confidential.

This means that documents not labelled with the classification level are to be considered "Unclassified" and therefore accessible to everyone without distinction, both inside and outside the company.
Documents present in the company but not produced internally, and therefore not labelled, must still be classified and be subject to the management methods indicated above, depending on the criticality of their contents.

4.2 Transfer and sharing of information with third-party companies

s.d.i. has defined the rules for sharing documents containing company information with third party companies. These rules take into account the criticality of the business information to be shared.

Documents shared with third-party companies classified as Highly Confidential s.d.i., Confidential s.d.i., must also indicate the name of the company with which the documentation in question is shared (e.g. Classification: Highly Confidential s.d.i. - Supplier XY / Classification: Confidential s.d.i. - Customer YZ).

In addition, each document shared with third-party companies must contain the following passage, as appropriate:

Classification Level: Highly Confidential / Confidential

In accordance with the International Standard ISO/IEC 27001, the data and information contained in all pages of this document are classified as Highly Confidential / Confidential / INTERNAL USE s.d.i.-[CUSTOMER/SUPPLIER NAME].

In order to avoid unauthorized access to the shared information, we ask you to observe scrupulous document management.

In the event of unauthorized disclosure of information (actual or suspected), the Management of s.d.i. must be ***promptly informed****.*

Documents shared with third-party companies classified as INTERNAL USE s.d.i. will instead contain the following wording:

Classification Level: Internal Use s.d.i.

In compliance with the International Standard ISO/IEC 27001, this document is classified as INTERNAL USE SDI; therefore it may not be reproduced, altered or disclosed by Third Parties.

4.3 Storage media and mobile devices

A process is defined for the management, allocation, replacement and destruction of PCs, laptops, removable devices, smartphones and any device that may contain data in order to avoid misuse of them and possible unauthorized disclosure of information. Storage media no longer in use must be stored, deleted or destroyed in a secure manner (e.g. low-level formatting).
Handling of data media should be done in a controlled manner to prevent unauthorized access or tampering with the information they contain.
Mobile devices must be adequately protected against unauthorized access. In particular, removable media must be encrypted. The assignment of the devices is recorded in a special register: these devices must be kept by the assignees with the utmost diligence to avoid the loss of information.

5. Physical security

Specific and adequate measures to guarantee physical security are identified and applied, including:

- Physical access control (e.g. reception entrance checks, entrance register, driveway control);
- Anti-intrusion systems and video surveillance system;
- Protected electrical supply systems (e.g. electrical cabinets, wiring, UPS);
- Fire-prevention systems (e.g. fire extinguishers, smoke detectors).
- Data redundancy on servers physically located in separate buildings and protected from natural or accidental events (e.g. fire).
- Data network redundancy (redundant fibre optic connection in copper with different paths to the operator).

The identification of the measures to be applied is based on the assessment of the criticality of the resources to be protected. The correct and periodic maintenance of the systems is ensured in order to guarantee their optimal operation and compliance with legal requirements. The identification and management of physical security measures, as well as their technical documentation, is ensured by the Physical Security Manager, with the possible collaboration of the Logical Security Manager.

6. Logical access control

s.d.i. s.p.a. adopts formal procedures to control the distribution of access rights to corporate information systems and for the management of user accounts, in all the phases of their "life cycle": from the creation of the user account, to its modification, updating, deletion.
Access rights to networks, systems, applications, data and corporate information are defined according to roles, the tasks performed and the actual work needs (on a "need-to-know" basis).
Administrator profile access rights to systems, networks and databases are limited and controlled and, where applicable, also in compliance with current legislation (as per Privacy Guarantor Provision on System Administrators). Users and access profiles to systems are periodically checked to verify adequacy over time and to remedy any non-compliant situations.
The methodology used by s.d.i. s.p.a. for the authentication of each user accessing IT systems is commensurate with the critical nature of the data contained in such systems, on the basis of which opportunities to use more secure authentication methods (e.g. strong authentication) are evaluated.
As a rule, the combination of user-ID and password is used, and the robustness of the secret authentication credentials is ensured by respecting the criteria of length, composition and periodic expiry.
A process is defined and implemented to ensure the timely deactivation of users no longer authorized to access the systems and information of s.d.i. s.p.a.
The identification and management of logical security measures, as well as their technical documentation, is ensured by the Logical Security Manager.

For remote access to the company network, encrypted VPN connections are used with access via user authentication and MFA based on mobile phone ownership.
The same level of authentication with MFA is provided for access to cloud services.

7. Management of information systems

In order to ensure the secure management of all company systems and infrastructures, rules and responsibilities must be documented with regard to:

- Installation of software on Servers, PCs and other corporate devices;
- Adjustment of the capacity of computing resources;
- Management of technical vulnerabilities and related patches;
- Security Threats Management;
- System backup;
- LOG collection and protection;

- Management of electronic and paper communications;
- Data transmission;
- Encryption of data, transmissions and communications in the cases provided for.

8. Software development and maintenance

Software development and maintenance processes must be properly regulated, documented and managed, not only with a view to pursuing the highest quality of service, effectiveness and operational efficiency but also with a view to ensuring that the software meets the necessary security requirements.

8.1 Application Change Management

The methods and responsibilities for managing activities relating to software development and maintenance are detailed in specific procedures. ~~In particular:~~

Throughout the software change process, the application of the defined security requirements must be tracked and controlled. The software must be tested. Tests must ascertain the smooth functioning of the security functions and the absence of vulnerabilities.

Furthermore, the separation of the development, test (possibly, integration) and production environments must be realised, also through the differentiation of the access privileges to the different environments, where necessary.

In the case of software development/maintenance services entrusted to third parties, the same development/maintenance management methods must be used and software security requirements must be applied as for internal developments.

In the case of developments by third parties, software acceptance criteria must also be defined.

8.2 Security requirements

Security requirements for software development and system modifications must be defined at an early stage of projects and documented.

8.3 Configuration management

Software storage and versioning shall be managed to keep track of the level of update of the systems and applications installed in the various environments. Previous software versions shall be retained as a preventive measure in case of failure of the new version.

8.4 Protection of source code and development environments

The source code of the programmes must be stored and protected against unauthorized access and accidental loss. Access to the source code and the development environments must be restricted to those persons responsible for modifying the applications, in accordance with the "need to know" principle.

8.5 Test data

Test data must be protected if they are complete or partial copies of production data or if they are critical. For this reason, access to development environments must be controlled and restricted, particularly if they are accessible by third parties.

9. Incident and problem management

Incidents shall be handled promptly and appropriately in order to minimise further damage and to restore normal operating conditions as soon as possible.
In particular, security incidents that may jeopardize confidentiality, integrity and availability of information must be identified. For this reason, an incident management process must be defined, documented and adopted that provides for at least:

- The classification of incidents according to their priority;
- The recording of incidents;
- Appropriate management arrangements in relation to classification;
- The identification of those responsible for resolving incidents;
- References for possible escalation;
- The analysis of reported issues;
- The use of an incident tracking tool;
- The preparation of appropriate reports;
- The periodic review of major incidents.

All employees and third parties are required to report incidents relating to s.d.i. s.p.a. information security through the channels and tools adopted in the company.

10. Business Continuity Management

Strategies and plans for business continuity and security should be adopted that take into account:

- Corporate services critical to the business;
- Minimum recovery requirements;
- Major incident scenarios derived from international best practices;
- Impacts of the above scenarios on the company and consequent levels of risk.

The ISMS Manager shall ensure that the following are defined and updated:

- The list of critical services;
- Minimum recovery requirements;
- Risk scenarios;
- Impacts on the company;
- Recovery strategies;
- Continuity plans and procedures;
- Measures to allow resumption of the service.

In addition, the ISMS Manager undertakes to ensure:

- The dissemination, within and outside the company (to the extent necessary), of the plans and procedures to be adopted to ensure business continuity;
- The adequacy of contractual agreements with Suppliers regarding the management (timing and methods) of disaster situations, depending on their involvement in the provision of critical services;
- The existence, updating and periodic testing of business continuity plans and the related responsibilities for managing the response to the incident and restoring the service in accordance with the minimum requirements defined, to be shared among all the functions involved;
- The adequacy of solutions for business continuity (e.g. system redundancies, system resilience, alternative site availability, distribution of critical skills, etc.)

The information security requirements to be applied in crisis and incident situations (e.g. data access authorizations, etc.) are the same as those applied during normal operations. Similarly, the roles and responsibilities defined and assigned for the management of information security during normal operations are the same as those to guarantee the continuity of information security management during crisis and incident situations.

11. Management of suppliers

The level of security guaranteed by third parties (e.g. IT Suppliers, outsourcers, partners, etc.) must conform to the level of security applied by s.d.i. s.p.a., in order to avoid the products/services acquired from outside constituting an element of weakness for the security of the information.
A risk assessment of third parties must be carried out in advance and the responsibilities, specific conditions, security requirements and SLAs (consistent with the risk assessments) that third parties are required to comply with must be defined and included in the contract, especially in the case of ICT suppliers/outsourcers.

12. Compliance and Audits

s.d.i. s.p.a. operates in compliance with the applicable national and international laws, internal regulations, voluntary regulations adopted, contracts with external counterparties. Furthermore, s.d.i. s.p.a. guarantees the adequate availability of documentation and resources to allow the activities of internal and external auditors.

The standards adopted by s.d.i. s.p.a. are:

- UNI EN ISO 9001
- UNI EN ISO 14001
- ISO/IEC 27001
- BS OHSAS 18001.

The Cyber Security standards of reference in the development of s.d.i. products (SCADA systems and automation and control equipment) are:

- IEC 62351
- IEC 62541

- IEC 61784-3
- IEC 62443

The following standards are also taken into account:

- NIST SP 800-82
- NIST SP 800-53
- NIST SP 800-57

In particular, for Functional Safety systems, the following standard is adopted:

- IEC61508:2010

The main mandatory regulatory references correspond to:

- Privacy legislation (Regulation (EU) 679/2016 and Privacy Code harmonised with the Regulation);
- Provisions of the Garante della Privacy ("Italian Data Protection Authority") applicable to the Company~~, in particular:~~
- Italian Legislative Decree 81/2008 (Consolidated Law on Safety at Work) and subsequent amendments;
- Italian Legislative Decree 231/2001 (Regulations on the administrative liability of legal persons, companies and associations, including those without legal personality) and subsequent amendments.

In addition to the above regulations, with specific regard to the electronic equipment produced and the electrical panels supplied, the references are as follows:

- CE marking: application of the procedures for verifying conformity and production of the product with the necessary documentation and manuals, affixing of the CE marking in the cases envisaged, preparation of the declaration of conformity following successful completion of the final checks and tests, including functional and electrical tests conducted with the appropriate certified equipment.
- UL certification (cULus): voluntary certification mark relating to product safety standards, recognised in North America (USA and Canada).

s.d.i. s.p.a. employs experienced internal professionals to ensure the implementation of regulatory updates. If necessary, s.d.i. s.p.a. uses external consultants who support the company on specific issues related to the sector's regulations.

The Function Managers of s.d.i. s.p.a. analyse the implications of new regulations on the area of their competence and ensure their application to the extent of competence.

The ISMS Manager plans periodic internal checks to verify compliance with and the correct implementation of this policy and the procedures of the Information Security Management System, agreeing on the possible need and planning of external audits with the corporate Functions concerned.