Management System

Information Security Policy

Rev	Date	Description	Written	Approved
0	31st May 2019	New emission	Cristina Giannelli Corporate IT Budget and Procedure Controller	Fabio Giannini Vice Corporate Finance Director

Sofidel Group, founded in 1966, with the Italian capital of Stefani and Lazzareschi families, is one of the world leaders in the production of tissue paper. His story is detailed on: http://www.SOFIDEL.com/en/SOFIDEL-group/our-history.

From its headquarter in Porcari (Lucca), Sofidel coordinates the activities of the group's companies in Europe and the United States (for an updated Group localisation see: http://www.SOFIDEL.com/en/SOFIDEL-group).

Information is considered a strategic asset for the company business and must be protected. Sofidel has therefore decided to set up an Information Security Management System and to guarantee an adequate level of data security in the design, development and provision, both internally and to subsidiaries, on ICT services, also through the identification, assessment and treatment of risks services are subject to.

Sofidel Information Security Management System defines a set of organizational, technical and procedural measures in order to guarantee the fulfillment of the basic security requirements listed below:

- Confidentiality, ie the ownership of the information, that has to be addressed only to authorized referents;
- Integrity, or information accuracy, the possibility of being modified only and exclusively by authorized referents;
- Availability, or the property of information to be accessible and usable when requested by processes and by authorized referents.

Management committment.

In order to provide the general and strategic direction in the short, medium and long term, to guarantee the protection of information in accordance with the indications of the UNI CEI ISO / IEC 27001 standard, Sofidel has developed the policy on the protection of corporate information assets described in this document.

To achieve the IT security objectives identified by the company management, an Information Security Management System must be established, implementing policies that the company intends to respect. The maintenance of this system is guaranteed by implementing a continuous process of improvement that involves all the corporate functions:

- Staff, who will implement the security policies and requirements to achieve the goals.
- The other companies of the group, considered customers for ICT Corporate. They will be guaranteed for their security needs.
- Suppliers, who will contribute, as partners, to the achievement of the organization's objectives, and will accept the security policies and the risks connected to the supply.

The Management is aware that the implementation of the Management System requires a significant initial effort and that maintenance and continuous improvement must be guarantee by adequate organizational support.

Changes has been made to Sofidel organization in order to define roles and responsibilities on Information Security, and IT Team will be able to operate according to this policy.

The Management will make the appropriate investments available to meet the established policies and objectives. The start-up of the System has been carried out with the support of external resources that have improved awarness on all aspects of information security.

Risk assessment and control framework

Information security requirements are valued by a systematic risk assessment using international standards.

The results of the risk assessment will led to the definitions of remediation plan in order to activate proper risks protection.

The risk assessment will be repeated periodically to address any changes that could affect the risk evaluation.

From the risk assessment results, an analysis of costs will take place, in order to balance benefits and risks.

Corporate Information Assets

Any type of data aggregation that has a value for the company, regardless of the form and technology used for their processing and storage, contributes to the formation of the company's information assets. The information must be protected in all the formats in which it is made available:

- Paper (documents, letters, lists, etc.)
- Electronic (databases, disks, tapes, etc.)
- Minutes (meetings, personal and telephone conversations, seminars, interviews, etc.)

Depending on the type and origin, the information that constitutes corporate information assets can be divided into:

- Information hosted in Customer's Information Assets (group companies), represented by the set of information managed by Sofidel through the ICT services provided. The security of this information must be guaranteed by contract and any security incident would have direct consequences on the image and development of the company business;
- Information managed in internal information assets, represented by all information within the company and partly managed through Information Systems. This information has influence over others and directly or indirectly affects all business activities.

The information must be evaluated to attribute its relative importance to the company business in order to implement adequate security measures proportional to the different forms and the different interaction methods used.

System implementation

This information security policy identifies the security aspects to be implemented within the organization in order to support Sofidel's mission and to pursue the following primary objectives:
The corporate functions responsible for information management and security are responsible for translating the aforementioned general objectives and requirements into more specific measures and security policies, with a view to obtaining an adequate Information Security Management System.
The primary objectives to be pursued according to the adopted security policy are the following:

- Compliance with current regulations
- Safeguard of the corporate image
- Business protection
- Compliance with contractual agreements

These objectives can be achieved by Sofidel through the collaboration of all the corporate structures that, each for the part of its competence, will set up a safety management system capable of:

- Guarantee the confidentiality, integrity and availability of information
- Evaluate risk levels
- Monitor security levels.
- To formalize the safety requirements in compliance with the mandatory regulation and the "best practices"
- Guarantee an adequate level of competence of the staff, reached with the necessary training and training and with the transmission of awareness of the importance of information security;
- Plan and manage business continuity;

The contents of the indications and the provisions of the system apply to all internal personnel, both within and outside the group, to partner companies, to suppliers and outsourcers and to anyone who comes into contact with Sofidel's own information.
All personnel who, as employees, consultants or collaborators, collaborate with the company in the processes of design, development, management and control of the services provided are responsible for complying with the requirements and indications of the system and are required to protect all the information processed during their work activities. The personnel, aware of the importance of the information processed must act to guarantee their protection and provide for the reporting of anomalies, even if not formally coded, which they should become aware of.

In the event that the established safety rules are disregarded by employees, consultants and / or collaborators, the Sofidel Management reserves the right to adopt, in full compliance with legal and contractual obligations, the most appropriate measures with respect to offenders.

External parties who have relations with Sofidel must ensure compliance with the security requirements set forth in this security policy, including by signing a "confidentiality agreement" at the time of assignment in the event that this type of restriction is not expressly mentioned in the contract.

The Information Security Policy must always be consistent with the corporate business objectives and therefore the Management reserves the right to make any changes to this document based on the achievement of Sofidel results to the expectations of all interested parties, to the performance of the reference market.
In accordance with the Information Security Policy and at least once a year, the Management will set the security objectives also using the results achieved during the previous year.

This policy has been approved by the Sofidel Company Management.

Date and Signature

Porcari, 31/05/2019

Fabio Giannini

Vice Corporate Finance Director