Corporate Policy Information Security

I. Introduction

Information is a strategic asset for the companies that make up the SEIDOR Group (hereinafter SEIDOR), as companies whose main activity is in the provision of Information Technology services, and therefore depend on IT systems (Information Technology) to achieve their strategic objectives. These systems must be managed with diligence, taking appropriate measures to protect them against accidental or deliberate damage that may affect the availability, integrity, confidentiality, authenticity, or availability of the information processed or the services provided.

The objective of information security is to guarantee the quality of information and the continuous provision of services, acting preventively, supervising daily activity, and reacting promptly to incidents.

IT systems must be protected against rapidly evolving threats that have the potential to impact the availability, integrity, confidentiality, authenticity, availability, intended use and value of information and services. Defending against these threats requires a strategy that adapts to changing environmental conditions to ensure continuous service delivery.

This implies that the security measures required by the Corporate Information Security Management System (ISMS), where the requirements of the Spanish National Security Scheme (NSS) are integrated, must be applied. SEIDOR continuously monitors the criteria and requirements established in the legislation that applies to it, such as Royal Decree 3/2010, of 8 January, which regulates the Spanish National Security Scheme in the area of Electronic Administration (ENS), Organic Law 3/2018, of 5 December, on Personal Data Protection and guarantee of digital rights (LOPDGDD), the European Union Regulation 2016/679 on the protection of personal data processing (GDPR) and internationally recognized standards such as ISO 27001 and ISO 20000-1, as well as to continuously monitor the levels of service provision, follow up and analyze reported vulnerabilities, and prepare an effective response to incidents to ensure the continuity of the services provided.

According to the information provided for by RD 3/2010 itself in Article 10, the existence of three distinct figures forming part, being:

- Responsible for the information will determine the requirements of the information processed.
- Responsible for the service Will determine the requirements of the services provided.
- Responsible for security Will determine the decisions to meet the requirements of information and service security.

SEIDOR must ensure that information security is an integral part of every stage of the IT systems life cycle, from conception to decommissioning, through development or acquisition decisions and exploitation activities. Security requirements and funding needs should be identified and included in planning, in the request for proposals, and in proposals for outsourcing IT projects.

II. Objective

•SEIDOR defines this Information Security Policy as a fundamental objective to guarantee the security of information and the continuous provision of the services it provides, acting preventively, supervising activity and reacting promptly to incidents that may occur.

This Policy must lay the foundations for the access, use, custody and safeguarding of the information assets used by SEIDOR to carry out its functions, to be carried out, under guarantees of security, in its different dimensions:

•Availability: property or characteristic of the assets consisting in that the authorized entities or processes have access to them when required.

•Integrity: property or characteristic consisting of the information asset not being altered in an unauthorized manner.

•Confidentiality: property or characteristic that the information is neither made available nor disclosed to unauthorized individuals, entities, or processes.

•Authenticity: property or characteristic consisting of an entity being who it claims to be or guaranteeing the source from which the data originated.

•Accountability: property or characteristic consisting of the fact that the actions of an entity can be attributed exclusively to that entity.

Under these premises the specific objectives of Information Security in SEIDOR will be:

•To ensure the security of information, in the different dimensions described above.

•To formally manage security, based on risk analysis processes.

•To draw up, maintain and test the availability and business continuity plans defined for the different services offered by the organization.

•To carry out an adequate management of incidents that affect the security of the information.

•Keep all personnel informed about security requirements and disseminate good practices for the safe handling of information.

•To provide the levels of security agreed with third parties when information assets are shared or transferred.

•Comply with current regulations and standards. The Security Policy:

•It will be formally approved by the General Management.

•It will be reviewed regularly, so that it can be adapted to new circumstances, techniques, or organizations, and avoid obsolescence.

•All employees and external companies who work with Seidor will be informed.

•Keep all personnel informed about security requirements and disseminate good practices for the safe handling of information.

•To provide the levels of security agreed with third parties when information assets are shared or transferred.

•Comply with current regulations and standards. The Security Policy:

•It will be formally approved by the General Management.

•It will be reviewed regularly, so that it can be adapted to new circumstances, techniques, or organizations, and avoid obsolescence.

•All employees and external companies who work with Seidor will be informed.

III. Mission

The purpose of this Information Security Policy is to protect SEIDOR information and services.

- SEIDOR expressly recognizes the importance of information, as well as the need to protect it, as it constitutes a strategic and vital asset, to the extent that it could endanger the continuity of the organization, or at least entail very significant damage, if there were to be a total and irreversible loss of certain data.
- SEIDOR implements, maintains and monitors the controls contained in its declaration of applicability and the ISMS processes, in accordance with the ENS, GDPR, LOPDGDD, ISO 27010 and ISO 20000-1 standards mainly, and complies with all applicable legal requirements.
- Information and services are protected against loss of availability, integrity, confidentiality, authenticity, and traceability.
- Service requirements regarding information security and information systems are met.
- The controls will be proportional to the criticality of the assets to be protected and their classification.
- The responsibility for the security of the information involved in the provision of the services included in the scope is that of the General Management, which will provide the appropriate means, without prejudice to the employees or users assuming their share of responsibility for the means it uses, as indicated in the policies, regulations and complementary procedures. The roles and responsibilities of the Cybersecurity Committee, which will manage information security, and of its members are described in point 6 “Organization of Security” of this document.
- Those in charge of Information Security and related security administration, will be the ones to manage the security.
- The people responsible for the information have been identified and must promote the establishment of controls and measures to protect the data that make up the information, especially those of a personal or critical nature.
- A system of information classification has been established within the regulations, with different levels.
- The necessary and adequate means have been established and made available for the protection of persons, data, programs, equipment, installations, documentation, and other media containing information, and in general, of any SEIDOR assets.
- The specific aspects most related to information on personal data are regulated by the set of rules contained in this security document and in the internal or other regulations to which it may refer, or which may be cited.
- The specific aspects most related to information on personal data are regulated by the set of rules contained in this security document and in the internal or other regulations to which it may refer, or which may be cited.
- Those who do not comply with these rules and the complementary procedures may be sanctioned in accordance with the labour legislation and the collective agreement of reference, or with personalized sanctions if they are linked to SEIDOR under non-labour contracts, in accordance with the clauses contained in such contracts and the legislation applicable in the latter case.
- Risk assessments are regularly carried out and, depending on the weaknesses, it is determined whether it is necessary to develop plans for the implementation or strengthening of controls.
- The dissemination of information and training in security to employees and collaborators is encouraged, preventing the commission of errors, omissions, fraud or crimes, and trying to detect their possible existence as soon as possible, and in case they exist, trying a very restricted dissemination of the inquiries.
- SEIDOR personnel should be aware of the rules and regulation standards and procedures related to their job, as well as their functions and duties, in addition to the separation of functions and the independent review of the records, when necessary, of who has done what, when and from where.
- Security incidents are communicated and dealt with appropriately.

IV. Scope

This Security Policy applies to all the companies that make up the SEIDOR Group and to their information systems and assets:

- To all departments, both their managers and employees.
- To contractors, clients or any other third party who has access to the organization's information or systems.
- To databases, electronic and paper files, treatments, equipment, supports, programs, and systems.
- To the information generated, processed, and stored, regardless of its support and format, used in operational or administrative tasks.
- To the information transferred within an established legal framework, which will be considered as its own for the exclusive purpose of its protection.
- To all systems used to administer and manage information, whether owned, rented or licensed by the company.