# ISSEL NORD
# INTEGRATED POLICY ON QUALITY AND SECURITY OF DATA AND INFORMATION

# Table of contents

## 1. FOREWORD

The Integrated Corporate Policy was developed on the basis of international standards which provide the requirements for an ISO 9001:2015 Quality Management System, EN 9100:2018 and an ISO/IEC 27001:2022 Data and Information Security Management System.

Issel Nord has structured its business processes adopting an in-house documented management organisational model in accordance with the requirements of UNI EN ISO 9001:2015, EN 9100:2018 and ISO 27001:2022, of which the Quality and Security of Data and Information Manual constitutes documented evidence.

Issel Nord complies with all legal regulations and at the same time ensures the monitoring of all risks and opportunities which may arise within the company processes, with a view to continuous improvement.

The Quality Management System and the Data and Information Security System represent Issel Nord's commitment to consolidate its core business and improve its performance.

The ISO 9001:2015, EN 9100:2018 Quality Management System and the ISO/IEC 27001:2022 Data and Information Security System aim to achieve the following objectives:

- ❑ Continuous improvement in the management of all processes;
- ❑ Achievement of a high level of effectiveness and efficiency in all activities performed, respecting the commitments entered into with stakeholders and at the same time complying with mandatory legal requirements.

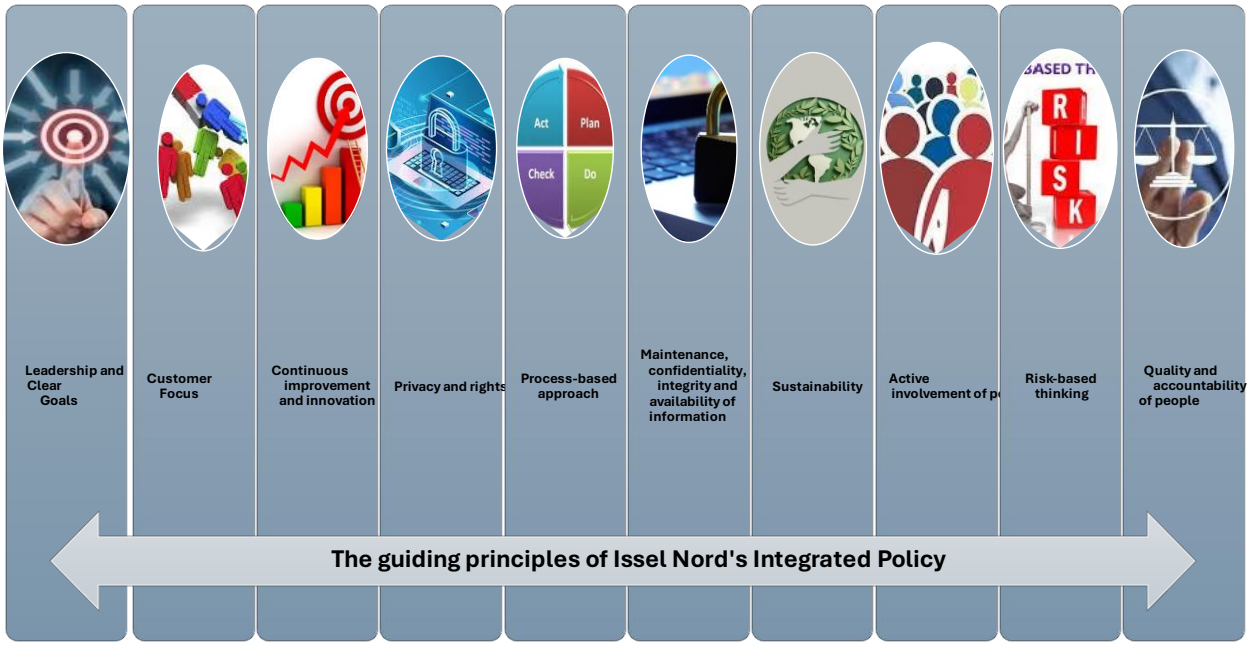
Management is committed to pursuing the objectives set and continuous performance improvement.

## 2. SCOPE OF APPLICATION

This Policy applies equally to all levels of the Company. The implementation of this policy is mandatory for all personnel and must be included in the regulation of agreements with any external party which, in any capacity, may be involved with the processing of information falling within the scope of the Data and Information Security Management System (DMS) and the Quality Management System (QMS). The company allows the external communication and dissemination of information only for the proper conduct of company business, which must take place in compliance with the rules and regulations.

## 3. THE GUIDING PRINCIPLES OF ISSEL NORD

Issel Nord adopts an integrated policy based on the guiding principles outlined below:




❑ Information is classified according to its level of criticality, so that it is managed with consistent and appropriate levels of confidentiality and integrity.

❑To ensure the security of information, access to the systems is subject to an identification and authentication procedure. Information access authorisations are differentiated according to the role and duties of individuals, so that each user can access only the information they require and are periodically reviewed.

❑ Procedures are defined for the secure use of company assets and information and their management systems.

❑ Full awareness of information security issues is encouraged in all personnel (employees and contractors) from the moment of selection and throughout the employment relationship.

❑ In order to be able to handle incidents in a timely manner, everyone must report any security-related problems using a ticket (TRACKIT) or by emailing helpdesk@isselnord.it. Every incident must be handled as outlined in the procedures.

❑ Unauthorised access to premises and individual company premises where information is managed must be prevented, and the security of equipment must be ensured.

❑ Compliance with legal requirements and information security principles in contracts with third parties is ensured.

❑ A continuity plan is in place to allow the company to deal effectively with unforeseen events, guaranteeing the restoration of critical services in a timeframe and manner that limits negative consequences on the company's mission.

❑ Security aspects are included in all phases of design, development, operation, maintenance, support and decommissioning of IT systems and services.

❑ Compliance with the provisions of the law, statutes, regulations or contractual obligations and any requirements concerning the security of information shall be ensured, minimising the risk of legal or administrative sanctions, significant loss or damage to reputation.

## 4. LEADERSHIP AND CLEAR GOALS

Management bears responsibility for the effectiveness of the Data and Information Security Management System (DMS) and the Quality Management System (QMS) and sets objectives that are compatible and consistent with the context and the strategic guidelines of the organisation.

Issel Nord's primary goals are:

- to constantly improve the quality of the products and services offered.
- to achieve and maintain a high degree of efficiency of activities within the company, with a view to preventing, reducing and, where possible, eliminating any anomalies, waste or other forms of non-compliance.
- to constantly improve the safety and quality management system for processes and products, also with the use of innovative technologies.
- to expand internal expertise to keep pace with future market trends.
- to achieve challenging goals and targets on a continuous basis, by implementing appropriate strategies.

Issel Nord’s constant commitment to the continuous improvement of the effectiveness of its Quality System, Data and Information Security System and its performance is secured through a structured programme of actions and objectives, on which periodic checks are performed. Issel Nord also pursues the continuous improvement of its Quality Management System and Data and Information Security System performances through control of its processes and the analysis of appropriate indicators of company performance and customer satisfaction.

Issel Nord is committed to implementing and maintaining sustainability-related initiatives through:

- Proper waste management;
- Use of recycled or biodegradable materials, where applicable;

- Reduced consumption of electricity, water, paper, toner cartridges and plastics;
- Reduced environmental impact;
- Sustainable mobility;
- The committed and responsible participation of its human resources, through the adoption of environmentally correct behaviour.

GSI STRATEGIC OBJECTIVES

- Ensure the security of data and information.
- Ensure a high level of IT system availability.

GSI INTERNAL TACTICAL OBJECTIVES

- Management defines the acceptable residual risk as 18%.
- Management guarantees network availability for 99% protection.

The objectives are assessed and monitored annually in the Review.

## 5. PROCESS-BASED APPROACH

The process-based approach, combined with the Plan-Do-Check-Act (PDCA) cycle, continuously and clearly improves the The Quality Management System and the Data and Information Security System.

## 6. MANAGEMENT COMMITMENT

Management actively supports Quality and Information Security in the company through clear direction, clear commitment, explicit assignments and the recognition of related responsibilities.

The management's commitment is implemented through a structure having the following tasks:

- ensure that all objectives relating to quality and information security are identified and that they meet corporate requirements;
- establish corporate roles and responsibilities for the development and maintenance of the QUA and GSI;
- provide sufficient resources for the planning, implementation, organisation, control, review, management and continuous improvement of the QUA and the GSI;
- check that the QUA and GSI are integrated into all business processes and that procedures and controls are effectively developed;
- approve and support all initiatives aimed at improving information security;
- activate programs for the dissemination of information security awareness and culture;
- periodically review the objectives emerged from the context analysis and the Risk Assessment and ensure the dissemination of these objectives to personnel through

periodic meetings (briefings) between departments, aimed at sharing and exchanging information with a view to continuous improvement;

- protect the company's information assets, including data and information relating to customers and suppliers, from threats that could generate significant risks, and provide evidence that the services provided do not cause an increase in information security risks;
- ensure an appropriate analysis of the service and confidentiality requirements of existing contracts in order to organise and develop the activity according to the client's requirements.

Senior Management approves the Quality and Data and Information Security Policy and, through it, ensures:

- **the protection** of data and information from unauthorised access;
- **the confidentiality** of data and information;
- **the availability of data** and information for the maintenance of corporate business processes;
- compliance with EU Regulation No. 2016/679 on data protection (GDPR), the provisions of the Data Protection Authority, the implementing decrees of the Jobs Act, the Privacy Law" Italian Legislative Decree 196/2003 and Italian Legislative Decree No. 24/2023 (transposing EU Directive No. 1937/2019 - so-called "Whistleblowing Directive");
- the planning, execution and control of the company's business;
- **personnel training** on data and information security management and the application of the GDPR;
- the recording and management of all data and information security breaches;
- the periodic conduct of a **specific analysis of the risks** to both data and all other aspects of the organisation that are related to data and information security.
- that all personnel are made **responsible** for the obligation to:
  - ensure compliance with the applicable rules, laws and regulations of a mandatory, contractual and voluntary nature made applicable in the areas of the GSI;
  - protect the confidentiality, integrity and availability of information managed by Issel Nord, its intellectual property and assets
  - protect Issel Nord's material assets, systems and resources;
  - safeguard and appropriately manage all data and information pertaining to their activities.

The information assets to be protected consist of all the information managed through the services provided and located in all the company's locations.

Issel Nord ensures:

- **confidentiality of information**: i.e. information must be accessible only by authorised persons.

- **integrity of information**: i.e. protecting the accuracy and completeness of information and the methods for processing it.
- **availability of the information**: i.e. that authorised users can actually access the information and related assets when they request it.

Lack of adequate levels of security can lead to damage to the company's image, lack of customer satisfaction, the risk of incurring penalties for violating regulations, as well as economic and financial damage.

An adequate level of security is also fundamental for sharing information.

## 7. OVERVIEW OF THE ORGANISATION

The external factors relevant to the maintenance of the Management System (GSI) and the Quality Management System (QUA) are:

- cultural, social, political, financial, economic, and competitive environment;
- customers;
- subcontracting and suppliers;
- applicable binding regulations and regulatory references;
- municipal administration where the company is located;
- Parent Company.

The relevant internal factors are:

- policies adopted (quality and data security);
- strategic and operational goals;
- technology used;
- employees with their roles and responsibilities, skills, and expertise.

## 8. RISK-BASED THINKING

For Issel Nord, risk-based thinking is essential to pursue effective Quality Management System and Data and Security System. Risk-based thinking comes into play both when analysing the risks associated with the business processes identified and when analysing operational risks.

## 9. QUALITY AND RESPONSIBILITY OF PEOPLE

Issel Nord undertakes to adapt and maintain over time its assets and employees (and the relevant training) to comply with the needs of the System. Issel Nord requires its employees to actively cooperate at all levels to implement the Quality and Data Security project and to implement the contents of the Quality and Data Security Manual.

Issel Nord commits to define responsibilities clearly, and to allocate them in a manner fully compatible with contractual clauses.

Issel Nord is committed to stimulating, encouraging, and recognising the contributions made by its personnel.

It has established common values and ethical standards at all levels of the organisation.

## 10. CUSTOMER FOCUS

Customer focus means meeting the customers' needs and future expectations, and Issel Nord achieves this through:

- the design, development, production, and testing of its products, as well as the continuous improvement of its key processes to achieve its goals of effectiveness and efficiency, after defining and addressing the risks and opportunities;
- full compliance with contractual specifications;
- a focus on increasing the quality level of its products and/or services.

## 11. CONTINUOUS IMPROVEMENT and INNOVATION

Issel Nord is constantly striving to implement continuous improvement actions, and to disseminate this principle among all those involved in company processes.

From the strategic perspective of development, competitive advantage and innovation, Issel Nord aims to:

- consolidate the tight relationship between technological innovation and strategic innovation;
- implement process innovations, understood as improvements to its production processes;
- seek new markets to obtain further competitive advantage.

## 12. ACTIVE INVOLVEMENT OF PEOPLE

Issel Nord believes in fostering employee retention by paying constant attention to the involvement of its employees in company projects, improvement processes and the achievement of pre-established goals, sharing objectives and results with its employees.

## 13. STATEMENT OF APPLICABILITY

Issel Nord has issued the Statement of Applicability in which the Annex A controls of ISO 27001 in force are listed.
The company identifies all security needs by means of a risk analysis to gain awareness of the level of threat exposure of its information system. The risk assessment makes it possible to evaluate the potential consequences and damage that may result from failure to apply security measures to the information system and what the realistic likelihood of implementation of the identified threats is.
The results of this assessment determine the actions necessary to manage the identified risks and the most appropriate safety measures.

## 14. REVIEW

The Management verifies the effectiveness and efficiency of the Quality Management System and the Data and Information Security System periodically and regularly, or when significant changes occur in order to ensure adequate support for the introduction of all necessary improvements and in such a way as to favour the activation of a continuous process, by which the control and adaptation of the policy is maintained in response to changes in the corporate environment, business and legal conditions. The review verifies the status of preventive and corrective actions and adherence to the policy and takes into account all changes that may affect the company's approach to information security management, including organisational changes, the technical environment, the availability of resources, legal, regulatory or contractual conditions and the results of previous reviews. The outcome of the review should include all decisions and actions related to improving the company's approach to information security management.

## 15. PRIVACY

The founding principles adopted by Issel Nord in the implementation of its Data and Information Security Management System, *with specific reference to the area of Privacy*, incorporate the core values set out in Article 5 of the GDPR, which require:

- *Lawfulness, transparency and fairness* in the processing of personal data, which may also be manifested through the explicit consent of the data subject, where the fulfilment of legal obligations or obligations arising from the performance of a contract, as well as the safeguarding of the vital interests of the individual and the explicit communications inherent in the processing are not in themselves sufficient to justify the purposes of processing. In this regard, Issel Nord takes appropriate measures to provide the data subject with all necessary information, including the purposes of the processing, the recipients of the personal data, the data retention period and the rights of the data subject, in a concise, simple and intelligible form;
- *Data minimisation*, which takes the form of using as little personal data as possible, depending on the purpose of the processing. With reference to the minimisation objectives, data must also be '*adequate, relevant and limited*' to what is actually required, without going beyond the purpose for which they were collected and processed;
- *Accuracy*, which requires compliance with the requirements of accuracy and updating, providing for the most appropriate operating procedures to enforce these principles;
- *Purpose limitation of the processing of personal data*, aimed at the collection and processing of information for specified, explicit and legitimate purposes;
- *Limitation of the storage of personal data* in such a way that the data subjects can be identified for a period of time not exceeding the fulfilment of the ultimate purposes for which they were collected and processed;

- *Integrity, confidentiality and availability*, through the use of technologies, processes and procedures aimed at deterring attempts at unauthorised access or use of personal data and the storage and archiving platforms used by the Company, also providing for timely reporting mechanisms to the competent Authorities if IT or physical breaches are detected on corporate archives.

Details concerning Issel Nord's data and information security management are contained in the following documents:

- Data and information security procedures based on ISO/IEC 27001 standards;
- Code of Ethics;
- Data Protection Impact Assessment report;
- Personal Data Processing Register (a record of processing activities carried out under one's own responsibility in which all information required by the GDPR is entered);
- Information Security Risk Analysis.

## 16. RESPONSIBILITY FOR COMPLIANCE WITH AND IMPLEMENTATION OF COMPANY POLICIES

Compliance and implementation of the policies are the responsibility of:

- All personnel who work in the company, in any capacity, and are in any way involved with the processing of data and information falling within the scope of the Data and Information Security Management System.
- All external parties that have relations and collaborate with the company must ensure compliance with the requirements contained in this policy.

Through appropriate rules and procedures, Management must:

- conduct risk analysis with the appropriate methodologies and take all risk management measures;
- establish all the necessary rules for the safe conduct of all company activities;
- verify security breaches and take the necessary countermeasures and monitor the company's exposure to the main threats and risks;
- organise training and promote personnel awareness for everything related to information security;
- periodically verify the effectiveness and efficiency of the Management Systems.

Anyone, whether employees, consultants and/or external collaborators of the company, who intentionally or negligently disregards the established safety rules and thereby causes damage to the company, may be prosecuted in the appropriate fora and in full compliance with legal and contractual constraints.

This Policy is a fundamental tool to raise awareness of the Quality and Data and Information Security principles throughout the organisation.

Follo,
01/07/2024

CEO

Documento firmato da:
SERGIO SEMPLICI
03.07.2024 15:48:06 UTC