INFORMATION SECURITY POLICY

Document code:	**POL-400_GRP_EN v08**
Approved by:	**Board of Directors Lutech S.p.a.**
Date:	**06/08/2026**

CLASSIFICATION

Public

TRANSLATION DISCLAIMER

This document is a translation of the original Italian text. In the event of any conflict, ambiguity or discrepancy between this translation and the original Italian version, the latter shall prevail and shall be considered the only valid and legally binding version.

CHANGE SUMMARY

Ver.	Date	Description of Changes
01	03/04/2018	First issue (POL-SGSI).
02	02/05/2019	Renamed to MSI-POL, revised content.
03	22/10/2020	General revision in content and form; inserted punctual references on ISO standards.
04	20/05/2022	Updated achievements.
05	11/03/2024	Amended version of the 27001:2022 standard.
06	25/05/2024	Updated PII definition with personal data instead of personally identifiable information.
07	27/03/2026	General revision of the MSI-POL contents and form; adoption of standard templates.
08	06/08/2026	General Review for NIS2

TABLE OF CONTENTS

1 INTRODUCTION

The Lutech Group's information assets are an essential strategic asset for the pursuit of corporate objectives, the provision of services, innovation, the protection of know-how and the creation of value for customers, partners and other interested parties. As a strategic asset, it must be adequately protected through a constant balance between the level of risk accepted and the level of protection required, combining the protection of information with the efficiency, effectiveness and continuity of business processes.

In a context characterized by increasing digitization, the evolution of cyber threats and the involvement of an increasing number of stakeholders, information security is a fundamental element to ensure the resilience of the Organization, the protection of information assets, the continuity of services and the maintenance of the trust of customers, partners and other interested parties.

2 PURPOSE

This Policy sets out the principles and commitments adopted by the Lutech Group to ensure the protection of the information and information assets processed in the context of its activities.

It establishes the framework to ensure the confidentiality, integrity and availability of information, in compliance with laws, regulations and contractual provisions, contributing to business continuity and the protection of business interests and customers.

This Policy also constitutes the reference for the definition and implementation of the organisational, procedural and technical measures adopted by the Group Companies in the field of information security.

3 SCOPE

This Policy applies to all Lutech Group Companies and all personnel, including collaborators, consultants, suppliers, partners and other third parties who, for any reason, process information or access the Group's information assets.

The Policy applies to all processes, products, services and information assets managed by the Group Companies and covers all information processed, regardless of the format, medium or technology used.

4 REGULATORY REFERENCES

- **ISO/IEC 27001:2022** - Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- **ISO/IEC 27002:2022** - Information security, cybersecurity and privacy protection — Information security controls
- **ISO/IEC 27005:2022** - Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- **ISO/IEC 27017:2015** - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- **ISO/IEC 27018:2025** - Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors
- **Directive (EU) 2022/2555 (NIS2**), where applicable;
- **Regulation (EU) 2016/679 (GDPR),** where applicable;

This Policy is adopted in compliance with the laws, regulations and contracts applicable in the countries in which the Group Companies operate and constitutes the common reference for the definition and implementation of information security measures.

The Group Companies ensure compliance with any specific regulatory requirements applicable according to the sector of activity, the jurisdiction to which they belong and the services provided.

5 MANAGEMENT COMMITMENT

Information security is a managerial and organizational responsibility and not exclusively technological.

The Management of the Lutech Group recognizes information security as a strategic priority and is committed to:

- guarantee adequate resources for the protection of information and information assets;
- defining roles, responsibilities and authorities in the field of information security;
- promote a corporate culture oriented towards security, awareness and empowerment of staff;
- ensure a systematic approach to managing information security risks;
- pursue the continuous improvement of security measures along the entire value chain;
- ensuring the resilience of essential processes and services;
- consider risks arising from the supply chain and third parties;
- ensure compliance with applicable laws, regulations, contracts and standards.

The Management also promotes the monitoring of the effectiveness of the security measures adopted and supports the continuous improvement of the level of information protection, in line with the evolution of the risk context and corporate objectives.

The Lutech Group's goal is to achieve and maintain a level of information security appropriate to the risks, consistent with the company's objectives and suitable for supporting the provision of reliable and resilient services.

The Group ensures compliance with the applicable laws, regulations and contracts, as well as the standards adopted, promoting the integration of information security into business processes and in the management of relationships with customers, suppliers and other interested parties.

6 CONTEXT AND STAKEHOLDER ANALYSIS

The Lutech Group periodically analyzes its operational, technological and regulatory environment, as well as the expectations of stakeholders, including customers, suppliers, partners, competent authorities, employees and other relevant stakeholders.

The analysis of the context makes it possible to identify the main risk factors and opportunities for improvement, adopting security measures proportionate to the nature of the services provided and with the acceptable level of risk.

The context analysis also considers the physical risks deriving from environmental and climatic events (e.g. extreme weather phenomena, energy outages, heat waves, floods), as potential causes of unavailability of ICT assets and services and interruption of business processes.

7 PRINCIPLES OF INFORMATION PROTECTION

The Lutech Group ensures that information is classified according to its value, criticality and level of sensitivity, adopting appropriate protection measures to ensure its confidentiality, integrity and availability.

Information and information assets are managed throughout their entire life cycle, from creation or acquisition to disposal, according to classification, protection, traceability and storage criteria, where applicable.

Access to information and information systems is allowed only to authorized users, according to the principle of least privilege and segregation of functions.

The Lutech Group adopts appropriate technical and organisational measures to prevent unauthorised access, undue disclosure, alteration, loss or destruction of information, including through the use of data and communication encryption techniques, where appropriate.

Security is considered throughout the entire life cycle of information systems, from design or acquisition to maintenance and decommissioning, promoting the adoption of security requirements from the initial stages and during all subsequent modifications.

Security vulnerabilities in assets and information systems are identified, assessed and dealt with promptly, depending on the level of risk and the evolution of threats.

The Lutech Group ensures that networks, communication infrastructures and network services are designed, implemented, managed and monitored according to the principles of security and resilience, adopting appropriate technical and organizational measures to prevent unauthorized access, interception, alterations, interruptions of services and other events that may compromise their security. Networks and communications are monitored in order to detect anomalies, threats and potential security incidents at an early stage. The methods for designing, managing, protecting and monitoring networks and communications are governed by operating procedures and technical standards adopted by the Group, depending on the risks and applicable regulatory requirements.

The Lutech Group prepares and maintains up-to-date business continuity, disaster recovery and emergency management plans, in order to ensure the resilience of services and the continuity of business activities.

Security events and incidents, as well as identified vulnerabilities, are promptly reported, analysed and managed in accordance with the provisions and procedures adopted by the Group.

8 RISK MANAGEMENT

Information protection is based on a structured risk management approach, aimed at identifying, analyzing, assessing and treating risks that may compromise the confidentiality, integrity and availability of information and information assets.

Information security decisions take into account the organizational context, the evolution of threats, the potential impact on business processes, information assets and services provided, adopting appropriate security measures proportionate to the level of risk.

Risk management also considers the risks arising from the supply chain and from third parties who, for whatever reason, process information or access the Lutech Group's information assets.

9 SECURITY IN CLOUD SERVICES AND PROTECTION OF PERSONAL INFORMATION

Ensuring compliance with the principles of data protection law and increasing customer trust in cloud computing technologies is a strategic objective for the Lutech Group. The same commitment specifically concerns the protection of PII (Personally Identifiable Information, i.e. Personal Data) or that of providing a structured way, based on privacy by design, to deal with the main legal issues, both legal and contractual, related to the management of personal data in IT infrastructures distributed following the public cloud model. The Lutech Group integrates these principles into the design, development, implementation, monitoring and improvement of cloud services, adopting organizational and technical controls appropriate to the protection of personal information.

10 OBJECTIVES AND KPIS

The Lutech Group defines information security objectives consistent with its corporate strategy and with the acceptable level of risk.

The Management identifies the following strategic objectives at Group level:

- Protect information from unauthorized access or disclosure (whether through deliberate or negligent actions);
- ensure the classification of information according to its value and level of sensitivity;
- ensure the integrity of information, preventing unauthorized changes;
- ensure the availability of information and services to support business processes;
- promote staff training, awareness and competence in information security;
- manage risks arising from the supply chain, ensuring that suppliers and partners adopt appropriate security measures for the services provided;
- promote the timely reporting, analysis and management of events, security incidents and vulnerabilities.

The achievement of the objectives is monitored by means of performance indicators (KPIs) and additional monitoring tools defined by the Group and periodically reviewed by the Management.

11 MANAGEMENT SYSTEM AND RESPONSIBILITIES

Information security is supported by a coordinated set of policies, procedures, technical controls and organisational measures and governance processes aimed at ensuring a level of protection appropriate to risks and consistent with the Group's objectives.

The Group Companies are required to comply with their information security activities with the applicable legislation, with the ISO 27001 (or equivalent) voluntary Information Security Management System, and with processes and procedures common to the Lutech Group.

Roles, responsibilities, authorities and levels of accountability in the field of information security are formally defined in order to ensure effective decision-making, coordination, control and supervision.

12 COMMUNICATION, TRAINING AND INVOLVEMENT

The Policy is communicated to all personnel and other parties who, in any capacity, operate on behalf of the Group Companies or access information and information assets

The Lutech Group promotes the training, awareness and awareness of its staff on information security, ensuring that the content is consistent with the roles and responsibilities assigned.

All recipients of this Policy are required to operate in compliance with the Group's policies, procedures and security provisions, confidentiality obligations and responsibilities assigned according to their role.

Awareness, empowerment and active involvement of all stakeholders are essential elements for the effectiveness of the measures adopted.

13 COMPLIANCE, MONITORING AND CONTINUOUS IMPROVEMENT

The Lutech Group periodically verifies the compliance of information security measures with the applicable legal, regulatory, contractual and internal provisions.

To this end, monitoring, verification and audit of information security are planned, aimed at assessing the effectiveness of the measures adopted, identifying non-conformities, areas for improvement and opportunities to strengthen the level of security.

The results of the verification activities are reported to the Management so that the appropriate decisions can be taken and corrective and improvement actions defined.

14 APPROVAL, REVISION AND VALIDITY

The Policy is subject to periodic review in order to verify its continued adequacy with respect to the evolution of the organizational, regulatory, technological context and threats to information security.

The Policy is also updated whenever there are significant changes to the internal or external context, applicable requirements, organization or services of the Lutech Group that may affect information security.

The Management promotes the periodic review of the effectiveness of this Policy and ensures its maintenance and continuous improvement.

15 LOCAL REQUIREMENTS

Lutech Group companies are required to apply this Policy in compliance with the laws, regulations and provisions issued by the competent authorities of the country in which they operate.

If local law provides for requirements that are more restrictive or additional than those defined in this Policy, such requirements shall prevail and shall be implemented through local procedures, standards or arrangements.