Politics

Integrated policy

Prepared by:	Michela Pecchia	Head of HR Organization & Learning Development	*Signed Michela Pecchia*
Validated by	Lorenzo Lombardi d'Aquino	Chief Human Resource & Organization Officer	*Signed Lorenzo Lombardi d'Aquino*
Verified by:	Marcello Vispi	Vice President	*Signed Marcello Vispi*
Approved by:	Renato Brunetti	Chairman & CEO	*Signed Renato Brunetti*

Summary

Revision Matrix

Rev.	Date	Prepared by	Validated by	Verified by	Approved by	Notes
0	09/04/2018	A. Spila			DIR	
01	01/18/2020	A. Spila			DIR	
02	03/25/2020	A. Spila			DIR	
03	11/11/2020	A. Spila			DIR	
04	03/09/2022	A. Spila			DIR	
05	01/23/2025	M. Pecchia	L. Lombardi d'Aquino	M. Vispi	R. Brunetti	
06	08/01/2026	M. Pecchia	L. Lombardi d'Aquino	M. Vispi	R. Brunetti	

1. INTRODUCTION

1.1. Premises and scope of application of the standard

The purpose of this document (hereinafter referred to as the Quality, Environment, and Information Security Policy) is to describe the general principles that UNIDATA has adopted in order to implement and maintain an efficient and secure Integrated Management System in accordance with the standards UNI EN ISO 9001:2015, UNI EN ISO 14001:2015, ISO/IEC 27001:2022 with extension to the requirements of the standards (guidelines) ISO/IEC 27017:2021, and ISO/IEC 27018:2020, ISO 45001:2018, PdR125:2022, and PAS 24000:2022.

These principles, as defined in Point 4.4. of the QM, are embodied in documented information specific to the System (such as the QM itself, Procedures, Operating Instructions, Regulations, and other documentation in use by the company - EL7.5.3A) for the purposes of maintaining a Quality Management System (QMS) and Information Security Management System (ISMS) as generically defined in Point 4.4 of the relevant "Manual", in relation to the actual needs arising from the type of activities carried out by Unidata in the specific scope of application of the aforementioned standards.

The aforementioned documented information shall be understood as supplemented by the documented information specific to the Privacy Organisational Model (MOP), applied by the Organisation in compliance with current and applicable national and European regulations on the processing of personal data, such as:

- EU Regulation 2016/679 - GDPR
- Legislative Decree 196/03 as amended by Legislative Decree 101/2018
- From the current provisions of the Privacy Guarantor, including, by way of example:
    - Measures concerning System Administrators
    - Measures concerning the processing of biometric data
    - Measures concerning data breaches
    - and others

and of which the Data Protection Policy document is an integral part.

The scope of application of the Quality, Environment, Gender Equality, and Social Management System (Points 1.3 and 4.3 of the MQ) and, consequently, of this Unidata Policy has been defined as follows:

Provision of Internet access, telephony, and data center services (cloud computing, hosting, housing, co-location, and security services) (IAF33). Design, installation, supply, and maintenance of telecommunications networks and local fiber optic networks and the Internet of Things operating through various transmission means and different applications (IAF28).

The scope of application of the Information Security System (Points 1.3 and 4.3 of the MQ) and, consequently, of the related Unidata Policy has been defined as follows:

Infrastructural management of the physical and logical security of its Data Center and related Facility Management and provision of Cloud services according to IaaS and PaaS models with the application of ISO/IEC 27017 and ISO/IEC 27018 guidelines in accordance with the declaration of applicability of June 5, 2020 (IAF 33)

In accordance with the declaration of applicability dated May 20, 2024

For the implementation of the aforementioned service provision activities, Unidata uses not only the operational infrastructure of its registered office but also the physical and logical infrastructure known as the Unidata Internet Data Center (hereinafter IDC), also located at Unidata's registered office at:

- **Rome, Viale A. G. Eiffel, 100 – 00148 Rome c/o Commercity Mod. M26**
- **Milan, Viale Edoardo Jenner 33**
- **Modugno (BA), Via delle Dalie 5**

The aforementioned infrastructure hosts data processing/management systems and equipment (generically referred to as "devices/servers") in environments equipped with appropriate physical and logical-IT security measures, as described below:

- **physical and/or virtual servers owned by Unidata** and directly dedicated to the operation of the IT systems necessary to ensure the management of the "company mission" ("vital" and/or "critical" company systems), i.e., the provision of "IT, Internet access, and other new generation" services to end users (customer base);
- **physical and/or virtual servers owned by Unidata, entrusted to end users/customers (Hosting)** for the operation of services outside the competence and responsibility of Unidata, which fall within the competence and responsibility of Unidata in relation to their correct functioning in operation and in relation to compliance with the obligations of monitoring, surveillance, and support in the suppression of crimes provided for by current national legislation;
- **physical servers owned by hosted customers (Housing)** at said infrastructure for the provision of services that are completely outside the competence and responsibility of Unidata and fall entirely and directly within the competence and responsibility of the user/customer entrusted with them;
- **areas (physical perimeters) leased exclusively to the user/customer (Co-location)** with or without access to the facilities referred to in the following point

The aforementioned premises pertaining to the IDC infrastructure, in addition to being equipped with suitable main

so-called "connectivity" services through the presence and availability of diversified "flows" aimed at managing data exchange on national/international networks with access to the Internet, also guarantee the following instrumental services (so-called "facilities"):

- access control system
- video surveillance system
- direct power supply system (primary power supply system) and indirect power supply system (backup power supply systems - UPS and uninterruptible power supply generator)
- air conditioning system and related alarm system
- fire and flood prevention system
- IT security systems (firewalling, antivirus, etc.)
- system monitoring and alarm systems
- system support and/or dedicated technical assistance (where contracted)

Through this infrastructure and through additional proprietary or third-party service infrastructures (physical and logical) distributed throughout the territory, end-user services are also provided, such as:

- Wired/wireless Internet access services, fiber optic (NGAN), copper, and radio (*hiperlan*)
- Fixed network voice telephony services using VoIP technology, remote and virtual switchboards, fax servers
- Data center services (housing, hosting, colocation, cloud, email, and more)

The following descriptions in this document and in the additional reference documentation for the Quality Management System and the Information Security Management System must therefore be understood as applying to the aforementioned physical-logical perimeter as well as to the related processes, resources, and/or working relationships (employees/collaborators/third parties with a legal interest) related and/or connected to the proper management of the aforementioned infrastructure within the broader and more general corporate objectives.

1.2. General Objectives of the IMS

The primary objective of an QMS is to achieve and maintain a continuously improving level of quality in the product/service delivery cycle for end users.

The primary objective of the ISM is to protect the data and elements of the information system responsible for their management.

In particular, pursuing information security means defining, achieving, and maintaining the following properties of the information:

- Confidentiality: ensuring that information is accessible only to duly authorized persons and/or processes;
- Integrity: safeguarding the consistency of information from unauthorized changes;

- Availability: ensuring that authorized users have access to information and associated architectural elements when they request it;
- Authenticity: guarantee the origin of the information;
- Non-repudiation: ensure that information is protected from false denial of receipt, transmission, creation, transport, and delivery.

The lack of adequate levels of security, in terms of Confidentiality, Availability, Integrity, Authenticity, and Non-repudiation, can lead, in any business activity, to damage to the company's image, customer dissatisfaction, the risk of incurring penalties related to the violation of current regulations, as well as economic and financial damage.

Information security is therefore a fundamental requirement for ensuring the reliability of the information processed, as well as the effectiveness and efficiency of the services provided by Unidata. Consequently, it is essential for the company to identify both external security requirements and those arising from legal obligations. This activity is carried out by drawing on various sources:

- Risk analysis: this allows the company to gain awareness and visibility of the level of risk exposure of its information system. Based on this level, appropriate security measures are identified. Risk assessment consists of the systematic consideration of the following elements:
  - damage that may result from the failure to apply security measures to the information system, considering the potential consequences of the loss of confidentiality, integrity, availability, authenticity, and non-repudiation of information;
  - realistic probability of how an attack could be perpetrated in light of the threats identified.

The results of the assessment help to determine the actions necessary to manage the identified risks and the most appropriate security measures in relation to the company's objectives, based on the definition of the level of residual risk that the company decides to accept, to be implemented subsequently.

The process of assessing and treating information security risks is conducted in accordance with the principles of the ISO/IEC 27001 standard, including the identification and assessment of assets, threats, and vulnerabilities, as well as the selection of appropriate security controls reported in the Statement of Applicability.

In light of the above, this policy, in compliance with the main regulations and standards on the subject:

- emphasizes the importance of ensuring the security of information and the tools used to process it;
- is consistent with the company's stated desire to ensure the protection of its information assets;
- addresses the physical, logical, and organizational aspects of the Information Security Management System.

In particular, Unidata's Quality, Environment, Gender Equality, Social and Information Security Policy is intended not only as a set of methodologies but also as managerial behavior, and is considered a strategic lever in all customer-oriented activities through the best use of human, financial, and technological resources. It is for this reason that UNIDATA proposes:

- the objective of ensuring complete customer satisfaction through the provision of quality services resulting from the standards defined in its Quality Management System.
- the objective of ensuring the secure management of information essential for business continuity and improvement, in line with and in compliance with the requirements of its Information Security Management System.

This Quality, Environment, Gender Equality, Social, and Information Security Policy is divided into the following general objectives:

- to develop and maintain a Quality Management System compliant with the UNI EN ISO 9001:2015, UNI EN ISO 14001:2015, PdR125:2022, and PAS 24000:2022 standards as a tool for achieving objectives, fulfilling commitments, promoting the continuous improvement of business processes, and ensuring compliance with mandatory requirements for related products and services;
- develop and maintain an Information Security Management System compliant with ISO/IEC 27001:2017, ISO/IEC 27017:2021, and ISO/IEC 27018:2020 as a tool for systematically and continuously monitoring processes relating to the security of all company information assets, not only from an IT perspective (electronic or paper media used to store documents and data) but above all from a management and organizational perspective, defining roles, responsibilities, and formal procedures to ensure the proper functioning of the company itself.
- adopt an integrated risk management system to ensure that the residual risk is minimized for all products/services provided;
- promote a culture of environmental awareness and eco-sustainable development;
- paying the utmost attention to special waste produced, ensuring maximum respect for the environment and current legislation;
- raising environmental awareness among key stakeholders (individuals inside or outside the company, with different interests and needs, who are able to influence the company's choices and behavior and affect its success).
- commit all available energy and capabilities to listening to customer feedback, suggestions, and desires, including through "on-field" activities;
- focusing every activity on customer needs in order to satisfy them better and faster, thereby establishing a leading position in the market;
- consolidate relationships with partners in order to provide customers with higher value, safe, reliable, high-tech products at reasonable prices;

- provide products and services that comply with all the requirements imposed by current legislation;
- spread appropriate culture and methodologies throughout the organization so that everyone who works there is constantly able to provide the best service expected by the customer;
- ensure a high level of satisfaction among all employees by seeking maximum loyalty and a sense of responsibility;
- encourage staff and management to realize their aptitudes, interests, and predispositions and develop their technical and organizational skills;

Management is committed to ensuring that these objectives are understood, accepted, and implemented at all levels of the organization through:

through:

- Direct, continuous, and ongoing commitment to the management of the Quality, Gender Equality, Social, Information Security, and Environmental Management Systems;
- Direct, full, and informed involvement and participation of company personnel at all levels in the implementation of the Integrated Management System;
- Establishing close collaboration and transparency with suppliers to improve the environmental impact of the products/services purchased;
- Commitment to legislative compliance in general and in particular in the environmental field, to pollution prevention and to continuous improvement;
- promoting an inclusive and equitable work environment that respects the rights of all employees, regardless of gender. The Company recognizes the importance of gender equality and is committed to creating equal opportunities and working conditions for all employees.

In particular, with regard to the EMS, According to Art. 5, paragraph c of Legislative Decree no. 152/2006, environmental impact is the qualitative and/or quantitative alteration, direct and indirect, short- and long-term, permanent and temporary, single and cumulative, positive and negative, of the environment, understood as a system of relationships between anthropic, physical, chemical, naturalistic, climatic, landscape, architectural, cultural, and economic factors, as a result of the implementation of plans or programs in the territory or the realization of projects relating to particular plants, works, or public or private interventions, as well as the commissioning of related activities.

Aware of the importance of environmental protection for its image and of its responsibilities towards the protection of the surrounding area, the Management has decided to adopt an Environmental Management System (EMS), Gender Equality and Social System to reduce the main environmental impacts and keep aspects related to its activities under control, thus taking an active role in protecting the environment.

Unidata S.p.A. also believes that it must assume responsibility within its sphere of operations for at least the following UN Sustainable Development Goals1 :

- the need for sustainable investment in the infrastructure necessary for the dissemination of communication technologies;
- the importance of promoting the smart city model to make cities inclusive, safe, resilient, and sustainable;
- promoting efficiency in the use of resources and energy;
- the need to take urgent action to combat climate change and its impacts;
- the need to protect, restore, and promote the sustainable use of terrestrial ecosystems, sustainable forest management, combat desertification, halt and reverse land degradation, and halt biodiversity loss.

This choice presupposes that the company's priority is to protect the territory, with a commitment to use the necessary resources with the utmost care and responsible environmental management according to a system aimed at continuously improving its performance.

In order to ensure the protection and well-being of its workers, as well as all stakeholders within its sphere of action and influence, Unidata undertakes to:

- comply with the principles adopted by international instruments such as the Universal Declaration of Human Rights, ILO conventions, other international standards, and national laws concerning human and labor rights;
- ensure consultation and participation of workers and workers' representatives;
- provide safe and healthy working conditions for the prevention of work-related injuries and illnesses, eliminating hazards and reducing OSH risks as determined by its own context analysis and OSH risk assessments;

Finally, in line with its purpose, the context in which it operates, and the strategic guidelines defined by senior management, Unidata adopts a Social Policy that integrates and complements this Integrated Management System Policy.

This Social Policy is based on respect for human rights, fair and safe working conditions, principles of corporate ethics and integrity, and the protection of health and safety at work for all workers and other relevant stakeholders.

Therefore, this Policy provides the framework for defining, reviewing, and updating social performance objectives, which are planned, monitored, and reviewed as part of the Integrated Management System and the Management Review process.

[1] United Nations General Assembly - New York, September 26-30, 2015

1.3. Operational objectives for the reference year

Senior management then defines and disseminates an annual plan containing the objectives for the year in question, which detail the general objectives involving the relevant levels and related corporate functions within the organization with the aim of increasing/improving the level of satisfaction of customers and other interested parties.

This document is identified as follows:

P6.2 Operational Objectives Plan

The Operational Objectives Plan also includes specific social performance objectives (e.g., relating to occupational health and safety, training on human rights and corporate ethics, industrial relations, and working conditions), consistent with the social aspects and commitments made by the Organization to workers and other stakeholders.

This Integrated Policy is reviewed and updated at least annually as part of the Senior Management Review (Point 9.3 of the Standard) and/or as required.

The lack of adequate product/service quality levels can lead, in any business activity, to damage to the company's image, customer dissatisfaction, the risk of incurring penalties related to the violation of current regulations, as well as economic and financial damage.

Quality is therefore a fundamental requirement for ensuring the reliability, effectiveness, and efficiency of the services provided by Unidata. Consequently, it is essential for the company to identify quality requirements both in inter-company relationships (employees/collaborators) and in external relationships (users/suppliers).

The results of the assessment help to determine the actions necessary to manage the risks identified and the most appropriate procedures and measures in relation to the company's objectives.

- **Guiding principles**: these are set out in Chapter 2 of this Policy entitled "Policy." They represent the system of values in which the company believes with regard to the quality management of its production/delivery system. These are the basic ideas that the company has developed with regard to quality, i.e., what is right or wrong to do in order to have a quality management system that is efficient, effective, and appropriate to its own needs and those of the market. The primary reference for the general safety principles is the UNI EN ISO 9001:2015, PAS24000:2022, PdR125:2022, and UNI EN ISO 14001:2015 standards.
- **Laws and contracts**: within the existing regulatory framework, guidance is provided on how to address issues related to maintaining a high level of quality in the provision of services to users, in the performance of related work tasks, and in relations with suppliers, collaborators, and technical and commercial partners. Compliance with Italian legislation on workplace health and safety, consumer protection, and fairness in professional and commercial relationships, as well as the constant pursuit of ethical objectives in these areas, serves not only to limit the risks of company involvement, but also to ensure an adequate level of quality in the company's production system.

This policy, in compliance with the main regulations and standards on the subject and in combination with the specific Data Protection Policy document:

- emphasizes the importance of ensuring the quality of the product/service and the tools used to achieve and maintain it;
- is consistent with the company's desire to ensure the satisfaction of the end user of these products/services;
- deals with the physical, logical, and organizational aspects of the Integrated Management System.

Senior management also undertakes to:

- **Disseminate and promote** the quality policy;
- **Implement** the quality policy by setting improvement objectives;
- **Review** the quality policy in light of the results achieved and company strategies.

and to ensure:

- information is protected from unauthorized access in accordance with confidentiality requirements and is available only to authorized users;
- information is not disclosed to unauthorized persons as a result of deliberate actions or negligence and, in accordance with integrity, is protected from unauthorized changes;
- business continuity plans are in place and that these plans are kept up to date and monitored as far as possible;
- staff receive training on information security;
- all information security breaches and possible weaknesses are reported to the appropriate authorities and investigated.

Through the implementation of this policy, Unidata intends to comply with UNI CEI ISO/IEC 27001:2017, UNI EN ISO 9001:2015, PdR125:2022, and PAS 24000:2022, UNI EN ISO 14001:2015, ISO/IEC 27017:2021, and ISO/IEC 27018:2020, as well as to achieve and maintain such certification. To achieve this objective, management is committed to ensuring that this policy is disseminated, understood, and implemented not only by internal staff but also by external collaborators and suppliers who are in any way involved with company information.

1.3.1. Regulatory references

- UNI EN ISO 9001:2015 "Quality Management Systems - Requirements."
- ISO 9000:2015 "Fundamentals and vocabulary of quality management systems";
- ISO 3100:2010 "Risk Management."
- ISO/IEC 27001:2017 Information security management systems – Requirements.
- ISO/IEC 27017:2021 "Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services,"
- ISO/IEC 27018:2020 "Information technology Security techniques Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors"
- UNI EN ISO 14001:2015
- ISO/IEC 27002:2017 "Information technology Security techniques Code of practice for information security controls"
- ISO/IEC 27701:2019 "Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines"
- ISO 45001:2018 "Occupational health and safety management systems – Requirements with guidance for use"
- PAS24000:2022 Social management system – specification
- PdR125:2022 Guidelines on the management system for gender equality

1.3.2. National and sector-specific regulations

- Legislative Decree 206/2005 Consumer Code
- Legislative Decree 259/2003 Electronic Communications Code
- Legislative Decree 196/2003 Personal Data Protection Code as amended by Legislative Decree 101/2018
- EU Regulation 2016/679 General Data Protection Regulation (GDPR)
- Legislative Decree 81/2008 and subsequent amendments Consolidated Law on Health and Safety in the Workplace
- ILO Convention No. 190 "Elimination of violence and harassment in the workplace: strengthens legal and other instruments to change the socio-cultural behavior of both men and women in order to eliminate prejudices, customs, and practices based on stereotypical gender roles."
- ILO Recommendation No. 206 Recommendation on violence and harassment
- Italian Constitution, Article 3 All citizens have equal social dignity and are equal before the law, without distinction of sex, race, language, religion, political opinion, personal and social conditions. It is the duty of the Republic to remove economic and social obstacles which, by limiting the freedom and equality of citizens, prevent

the full development of the human person and the effective participation of all workers in the political, economic, and social organization of the country.

1.4. Documented Information (Documents) of the SGQ

The list of documented information of the Unidata SGI, including any classification category, is contained in doc. EL7.5.3A. The list is supplemented by documented information relating to the Unidata Privacy Organisational Model (MOP).

2. POLICY

2.1. Quality Policy

The general principles that inspire Unidata's Quality Policy, defined by senior management in line with the context of the organization, relevant stakeholders, and strategic direction, form the framework for defining and reviewing quality objectives and other objectives of the Integrated Management System.

They are structured as follows:

- Ensuring that the requirements of customers and interested parties are well defined and a fundamental part of the proposed solutions;
- Ensure that the characteristics of the product or service offered are based on the principle of maximum information and transparency;
- Ensure clear and constantly improving delivery and maintenance processes;
- Always strive to provide customers with a service in line with the performance expressed in the Service Charter;
- Ensure that every level of the company acts in accordance with the commitments made in the Unidata Code of Ethics;
- Always bear in mind that the sole reason for Unidata's existence lies in the quality of its relationships and the quality of the services it offers to its customers;
- Ensure compliance with current legislation;
- Ensure compliance with the management system;
- Ensure the adequacy of the structure and equipment.
- Assess the impact of its activities and whether relevant stakeholders may have requirements that affect climate change;
- Identify the company's various activities as processes to be planned, controlled, and continuously improved; organize and monitor the resources involved in their implementation in the best possible way (process approach);
- Communicate the importance of ensuring the effectiveness and compliance of the QMS to all interested parties and actively involve them, coordinating and supporting them. In particular, Unidata's senior management is committed to constantly supporting the company's various management roles, highlighting the indispensable importance of their contribution to the improvement of the IMS (leadership);
- Assess and address risks associated with processes and the achievement of its strategic objectives; Exploit and reinforce identified opportunities (risk and opportunity assessment).

Based on these principles, within the scope of its IMS, Unidata

Undertakes:

- towards customers, to provide products and services that meet mandatory requirements and are of high quality, to demonstrate transparency and reliability, to ensure product quality at competitive prices through cost analysis and containment;
- towards suppliers, to promote a fruitful "alliance" so as to be an active part in defining product performance and characteristics, and to provide the necessary support for understanding and defining customer requirements and mandatory requirements relevant to the product;
- towards employees, to promote a spirit of initiative, encourage professional growth, ensure fruitful and peaceful professional relationships, and guarantee a safe working environment in which everyone can be satisfied;
- towards the owners, to promote the growth of the company, ensuring adequate profitability and financial stability, which are essential elements for the success of the quality policy.

aims to:

- develop and maintain an Integrated Management System as a tool for achieving objectives, fulfilling commitments, promoting continuous improvement of business processes, and ensuring compliance with mandatory requirements for related products and services;
- adopt an integrated risk management system to ensure that the residual risk for all products/services provided is minimized;
- commit all available energy and capabilities to listening to customer feedback, suggestions, and desires, including through "on-field" activities;
- focus every activity on customer needs in order to satisfy them better and faster, thereby establishing a leading position in the market;
- consolidate relationships with partners in order to provide customers with higher value, safe, reliable, high-tech products at reasonable prices;
- provide products and services that comply with all the requirements imposed by current legislation;
- spread the appropriate culture and methodologies throughout the organization so that everyone who works there is constantly able to provide the best service expected by the customer;
- ensure a high level of satisfaction among all employees by seeking maximum loyalty and a sense of responsibility;
- Encourage staff and management to realize their aptitudes, interests, and predispositions and develop their technical and organizational skills.
- Communicate and update quality guidelines, commitments, and objectives on an annual basis;
- Convene specific meetings periodically to ensure that the need to meet the requirements of contracts and specifications is understood and shared at all levels and to make the updates required by changes in mandatory regulations;
- Ensure that the objectives of the quality policy are defined and compatible with the context and strategic direction of the company and that they include information security;
- Ensure the integration of integrated management system requirements into company business processes.

- Communicate the company policy to all employees.

Aims to:

- develop service techniques designed and implemented to meet customer needs, anticipate expectations, and provide solutions that create value for the customer;
- systematically select new high-tech products;
- speed up the distribution of products and services by adopting the most innovative and reliable technical tools, making the organization more efficient and utilizing all the necessary potential.

Unidata's work complies with the following principles:

- Collaboration with certification bodies;
- Collaboration with customers.

2.2. Social policy and corporate social responsibility

Senior management, in coordination with the Steering Committee, defines, implements, maintains, and reviews a Social Policy that includes respect for human rights, the protection of decent, fair, and inclusive working conditions, respect for the principles of business ethics and integrity, and the protection of health and safety at work.

Unidata is committed to meeting all applicable legal requirements regarding labor, human rights, health and safety, non-discrimination, working hours, remuneration, and freedom of association and collective bargaining, as well as contractual requirements agreed upon with customers, suppliers, trade unions, and other stakeholders relating to social performance.

Where applicable national legislation provides for different levels of protection than the reference standards adopted by the Organization, the level of compliance that guarantees the greatest possible protection for workers shall apply.

The Social Policy provides the framework for defining, implementing, and reviewing the social performance objectives included in the Operational Objectives Plan, and is subject to continuous improvement through monitoring of results, internal audits, worker reports, and Management Review.

Senior Management ensures that the Social Policy is available as documented information in the Integrated Management System, is communicated, understood, and applied at all levels of the Organization, and is made available, where appropriate, to business partners, including suppliers and other interested parties, including through publication on company information channels and/or integration into relevant contractual agreements.

Finally, senior management is committed to establishing, implementing, and maintaining a structured process for consulting and involving employees and their representatives (RLS/RSU) at all levels and applicable functions, concerning the development, planning, implementation, performance evaluation, and improvement actions of the Social Management System.

This process provides for mechanisms, time, training, and adequate resources to ensure timely access to clear and relevant information, as well as the identification and removal of barriers to participation (such as language barriers, fear of retaliation, or lack of feedback on input).

In particular, emphasis is placed on consulting non-managerial workers to: determine the needs and expectations of interested parties; establish and review the Policy; assign roles, responsibilities, and authority; comply with legal and contractual requirements; set social performance objectives; define controls on outsourcing, suppliers, and contractors; determine monitoring and evaluation; plan internal audits; and ensure continuous improvement.

The active participation of non-managerial workers is also promoted in the assessment of social risks and opportunities, the definition of training needs, the determination of internal communications, the implementation of operational controls, and the analysis of incidents/non-conformities with corrective actions.

The results of consultations and participation are documented and integrated into the Management Review and continuous improvement processes of the Integrated Management System.

2.3. Gender Equality Policy

Unidata S.p.A. is committed to non-discrimination on the basis of gender in hiring, promotions, dismissals, and task assignments, basing decisions exclusively on merit and skills. It prohibits harassment, mobbing, and physical/moral violence (including outside the workplace) with zero tolerance, ensuring a safe environment free from discrimination.

It promotes inclusive language in all documents/communications and equal development opportunities for all employees. It offers work-life balance by supporting maternity/paternity leave with flexible working and gradual return to work, continuously improving working conditions in accordance with social responsibility.

It guarantees mandatory biennial training on gender stereotypes to eliminate prejudice, with specific courses for managers on leadership responsibilities. It implements a confidential reporting channel for violations, handling each case with impartial investigations and appropriate sanctions.

It dedicates an annual budget to equality objectives, continuously monitoring the effectiveness of the policy through KPIs, internal audits, and management reviews. It provides written instructions, ethics training, and periodic reviews for continuous improvement, integrating equality principles into the Integrated Management System.

All levels of the company are responsible for implementation, maintaining relationships based on mutual respect, equality, and personal dignity.

Unidata has established a Steering Committee and appointed its members, with the task of coordinating the drafting of the Strategic Plan and company policies. It has also identified a competent resource for the management of the Gender Equality system.

In addition,

- It is actively committed to family welfare, providing concrete support to the families of its employees both in economic terms and in terms of flexible working hours and agile working;
- It supports events aimed at promoting gender equality and inclusion;
- Promotes active policies for gender equality and inclusion through posts and publications on social media

2.4. General principles of environmental management

The general principles that inspire Unidata's Environmental Policy, specifically in the field of application of the Unidata IMS referred to in Point 1.1, are as follows:

- implementing all possible pollution prevention measures, taking into account the tangible and intangible resources available within the Company, each actor in the supply chain, and each stage of the life cycle of the product used and the service provided;
- raising employee awareness through appropriate information and training programs, so that staff at all levels ensure the effective application of the Environmental Management System within their areas of responsibility, adopting behaviors inspired by green-office principles;
- promote and disseminate an "environmental" culture to all stakeholders, including customers, partners, suppliers, etc.;
- take environmental performance criteria into account in the supplier qualification and evaluation process;
- promote "Smart Working," encouraging sustainable mobility for employees and collaborators;
- favor sustainable and/or eco-friendly purchases;
- encourage recycling and recovery;

2.5. General principles of health and safety in the workplace

The general principles that inspire Unidata's Health and Safety Policy in the workplace, specifically in the field of application of the Unidata IMS referred to in Point 1.1, are as follows:

- monitoring the Company's application of and compliance with OHS regulations in relation to interested parties through specific control methods and tools;
- promoting the involvement and participation of workers, and in particular workers' representatives, in the process of risk assessment and OSH hazard mitigation;
- raising awareness among employees through appropriate information and training programs so that staff at all levels ensure the effective application of the OHS Management System within their responsibilities and are able to monitor *near misses* in order to prevent accidents, incidents, and occupational diseases;

- ensure the involvement and dialogue between the key figures of the two Management Systems: Corporate Social Responsibility and OSH;

2.6. General principles of Information Security

The general principles that inspire Unidata's Information Security Management Policy, specifically within the scope of application of the standard referred to in Point 1.1, are divided into the following topics:

- Identification, classification, and management of resources
- Secure management of logical access
- Rules of conduct for the safe management of company resources
- Personnel and Safety
- Management of abnormal events and accidents
- Physical security management
- Contractual aspects related to information security
- Business continuity management
- Monitoring, tracking, and technical checks
- System and service lifecycle
- Compliance with regulations

Cybersecurity risk management is integrated into corporate risk management processes. The Organization defines and maintains a cyber risk management plan, including identification, analysis, assessment, treatment, and continuous monitoring of risks associated with critical services.

The information security objectives deriving from this Policy are translated into specific and measurable objectives within the Operational Objectives Plan and the ISMS documentation, and their achievement is monitored regularly through appropriate performance indicators and audit activities.

Below are the objectives and guidelines defined by Unidata for each topic.

2.6.1. Identification, classification, and management of resources

Objective: *All Unidata staff and, where relevant, collaborators must receive adequate awareness-raising, education, training, and periodic updates on organizational policies and procedures relevant to their activities.*

- A system for recording all tangible and intangible assets to be protected (information, hardware, software, paper documentation, and storage media) must be in place and kept up to date over time.

- Each resource (tangible/intangible asset) must be directly associated with a responsible company department.
- Information must be classified according to its level of criticality, so that it can be managed with consistent and appropriate levels of confidentiality and integrity. The criticality of information must be assessed as objectively as possible, using appropriate working methods.
- The management methods and protection systems for information and the assets on which it resides must be consistent with the identified level of criticality.

The Organization maintains an up-to-date inventory of critical assets, systems, and services, ensuring their traceability and availability for operational resilience purposes.

2.6.2. Secure management of logical access

Objective: *To ensure secure access to information in order to prevent unauthorized processing or viewing by users who do not have the necessary rights.*

- Access to information by each individual user must be limited to only the information they need to perform their duties (the "need-to-know" principle). The communication and transmission of information internally, as well as externally, must be based on the same principle.
- Access to information in digital format by authorized users and systems must be subject to the completion of an identification and authentication procedure.
- Authorizations to access information must be differentiated according to the role and duties of each individual and must be reviewed periodically.
- A process for managing authorization credentials and related access profiles must be defined.
- The systems that make up the ICT infrastructure must be adequately protected and segregated in order to minimize the possibility of unauthorized access.

2.6.3. Behavioral rules for the secure management of company resources

Objective: *To ensure that Unidata employees and collaborators adopt behavior patterns aimed at ensuring adequate levels of information security.*

- Work environments and company resources must be used in a manner consistent with the purposes for which they were made available and ensuring the security of the information processed.
- Procedures must be defined for the management and use of information in both digital and paper form.

- Company IT systems must be used by employees and collaborators in accordance with approved procedures.

2.6.4. Personnel and security

Objective: To ensure that personnel working on behalf of Unidata (employees and collaborators) are fully aware of issues relating to information security.

- During the selection and induction of personnel at Unidata, their level of knowledge of company security objectives and issues must be assessed in relation to the activities they will be performing.
- During their time at Unidata, personnel must receive adequate and ongoing training on data security issues.
- The procedures for terminating employment with Unidata must be consistent with corporate security objectives.

Management ensures that personnel with managerial and decision-making responsibilities, including members of senior management, receive periodic training specific to cyber risks.

2.6.5. Management of abnormal events and incidents

Objective: *To ensure that anomalies and incidents affecting the information system and company security levels are promptly recognized and correctly managed through efficient prevention, communication, and response systems in order to minimize the impact on the business.*

- All employees and collaborators are required to identify and report any issues related to information security to the appropriate person in charge, following the appropriate procedures.
- Incidents that may have an impact on security levels must be detected and any damage, potential or otherwise, must be managed as quickly as possible in accordance with specific procedures.
- There must be a system for recording and classifying incidents and abnormal events in order to carry out analyses aimed at improving security levels in line with the actual problems encountered.

Unidata guarantees the management and timely communication of security incidents, ensuring the ability to provide preliminary, intermediate, and final notifications to the competent bodies, according to the established timelines.

2.6.6. Physical security management

Objective: *To prevent unauthorized access to company premises and individual rooms and to ensure adequate levels of security for the areas and assets through which information is managed.*

- The security of areas and premises must be managed by:
  - the identification of areas and the classification of premises based on the criticality of the information processed;
  - the definition of adequate levels of protection;
  - the establishment of a periodic cycle of checks and controls.
- The security of equipment must be ensured by:
  - the definition of an appropriate location for information processing equipment;
  - the provision of the resources necessary for their operation;
  - the provision of an adequate level of maintenance;
  - the establishment of a periodic cycle of checks and controls.

2.6.7. Information security management for cloud services

Information security management for IaaS and PaaS cloud services provided by Unidata is set up in accordance with the guidelines of the ISO/IEC 27017 standard, in order to clearly and transparently define the responsibilities of the cloud service provider and the customer, as well as the specific security controls applicable to the cloud environment.

Cloud service customer	Cloud service provider (Unidata)
The cloud service customer is properly informed about all aspects of the following: - Information stored in a cloud computing environment may be accessed and managed by Unidata; - Resources may be maintained in a cloud computing environment, for example, application programs; Cloud service administrators have privileged access.	Unidata provides guarantees regarding the following aspects: - Basic information security requirements applicable to the design and implementation of the cloud service - Risks from authorized insiders - Access to customer cloud service activities by Unidata personnel - Guarantee regarding access control procedures - Prompt communication during change management - Data protection assurance - Management of customer account lifecycle

	- Communication of breaches and guidelines for sharing information to support investigations and forensic analysis - Guarantee, to the extent of its competence, the implementation of security controls specific to the cloud environment, such as logical segregation between different *tenants*, secure management of accounts and privileged access, protection and management of cryptographic keys, and definition of the locations of processed data.

2.6.8. Contractual aspects related to information security

Objective: *To ensure compliance with legal requirements and principles related to information security in contracts with third parties, in accordance with the specific characteristics of the relationship that Unidata must establish with those third parties.*

- Agreements with third parties and outsourcers who access information and/or the tools that process it must be based on formal contracts containing appropriate security requirements.
- Agreements with third parties and outsourcers, where necessary, must ensure compliance with legal requirements regarding the protection of personal data ("privacy regulations").

Unidata applies specific security requirements to the supply chain, with particular attention to suppliers that affect essential or critical services. This includes periodic assessments of critical suppliers, contractual security requirements, compliance checks, and continuous monitoring of relevant dependencies.

2.6.9. Business Continuity Management

Objective: *To ensure the continuity of Unidata's business and the timely restoration of services affected by serious abnormal events, reducing the consequences both inside and outside the company.*

- All events that could lead to a disruption in business continuity must be carefully identified and assessed in terms of probability of occurrence and possible consequences.
- A continuity plan must be put in place to enable the organization to deal with the consequences of an unforeseen event in an organized and efficient manner, ensuring the restoration

of critical services in a timely manner and in a way that minimizes the negative impact on the company's mission.

- All operational and organizational procedures necessary to ensure the implementation of the continuity plan must be prepared, validated, and appropriately disseminated.
- Tests must be carried out periodically for all components of the continuity plan.
- The plans and procedures referred to in the previous points must be maintained and updated in order to ensure the effectiveness of the system over time in the face of any organizational/technological changes.

Business continuity and disaster recovery plans are structured to ensure operational resilience, guaranteeing that critical services can be restored according to service levels compatible with identified internal and external dependencies.

Points of the Standard: 17.1, Annex A - ISO/IEC 27001:2017

2.6.10. Monitoring and tracking of technical audits

Objective: *To ensure the detection of abnormal events, incidents, and vulnerabilities in information systems in order to guarantee the security and availability of services and related information.*

- Information systems must be periodically checked in order to assess the correct functioning of the security systems, hardware, and software implemented, as well as the possible presence of vulnerabilities not detected or known in the past.
- Based on the results of all monitoring, tracking, and verification activities, periodic analyses must be carried out to identify critical areas and appropriate corrective and improvement actions.
- Periodic audits of the information security management system must be planned.

2.6.11. System and service lifecycle

Objective: *To ensure that security aspects are included in all phases of the design, development, operation, maintenance, support, and decommissioning of IT systems and services.*

- Security aspects must be given due consideration during the design and development phase. In particular, the following issues must be addressed:
  - inclusion of security requirements in the functional specifications of services and systems;
  - adoption of best practices for software development and maintenance;
  - controlled documentation management;

  - separation of development and testing environments with the use of formal acceptance procedures when moving between environments.
- During the operational phase, security aspects must be given due consideration. In particular, the following issues must be addressed:
  - capacity management of the technological infrastructure;
  - system and data security (configuration management, hardening, installation of anti-malware systems, encryption);
  - use of change management procedures;
  - adoption of backup and restore procedures;
  - adoption of controlled system decommissioning procedures (e.g., secure disk erasure);
  - Network security: network segregation, gateway monitoring (firewalls).
- Security aspects must be taken into account in the management of services. In particular, the following issues must be addressed:
  - system and service monitoring;
  - user management;
  - performance monitoring.

2.6.12. Compliance with regulations

Objective: *To ensure compliance with the provisions of the law, statutes, regulations, or contractual obligations and all requirements relating to information security, minimizing the risk of legal or administrative sanctions, significant losses, or reputational damage.*

- All regulatory and contractual requirements relating to information system security and impacting the Information Security Management System must be identified and analyzed in order to assess their impact on the organization and information systems.
- The managers of the various areas must ensure, each within their own area of responsibility, that all policies, procedures, standards, and in general all documentation relating to information security are applied and complied with.
- Failure to comply with the provisions of this document and all other documents derived from it will be handled in accordance with the provisions of the National Collective Labor Agreement or, in the case of non-compliance by third parties, in accordance with existing contractual relationships.

2.6.13. Security of data managed through Iaas, PaaS, and SaaS services sold

The company has always made information security and protection a cornerstone of its systems.

In addition to all the systems for protecting data from external attacks, backing it up, and state-of-the-art disaster recovery systems, Unidata has decided to adopt a comprehensive system of security measures, management procedures, and a documentation system that complies with national and European requirements regarding the processing of personal data (Data Protection Policy - General and specific security measures) and with the requirements of voluntary certification standards (ISO/IEC 27001; ISO/IEC 27017 and ISO/IEC 27018) as a synergistic integration, calibrated to the nature of the services provided to customers, to the management systems already in place.

In the event that, as part of the cloud services provided, Unidata processes personal data on behalf of customers, the Organization acts as data processor and applies the principles and controls set out in the ISO/IEC 27018 standard for the protection of personally identifiable information (PII) in public cloud environments.

In particular, Unidata undertakes to:

- process personal data exclusively on the basis of documented instructions from customers and only for the purposes authorized by them;
- adopting appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of PII processed in cloud services;
- ensure that any sub-suppliers processing PII on behalf of Unidata are selected and managed through agreements that provide for at least equivalent levels of security and protection;
- support Customers in fulfilling their obligations under personal data protection legislation, including the management of requests to exercise the rights of data subjects, within the limits of the responsibilities and technical capabilities of the services provided;
- define and apply procedures for the secure return and/or deletion of PII at the end of the contractual relationship or at the customer's request, without prejudice to any different legal requirements.

These provisions are supplemented and detailed in the "Policy for the protection, access, and integrity of data relating to processes and procedures" and in the remaining documentation of the Privacy Organizational Model (MOP), which form an integral part of the Information Security Management System.

3. DEFINITION OF ROLES AND RESPONSIBILITIES

3.1. Responsibility for the management system

Management assumes responsibility for establishing and disseminating the Environmental Policy both within and outside the Company, ensuring that it is:

- documented, understood, supported, implemented, and communicated to all personnel;
- available to anyone who requests it.
- communicated to business partners, suppliers, and other relevant interested parties.

UNIDATA SPA constantly analyzes the interactions of its activities with the context and, in order to keep the Environmental Management System active and dynamic, annually prepares a system of measurable objectives and targets using indicators and a monitoring program to ensure the effectiveness and efficiency of the system itself. The analysis of the data provides useful information for the subsequent definition of interventions and actions aimed at preventing or mitigating the most significant aspects that have emerged.

Management is personally involved in complying with and implementing these principles, ensuring and periodically verifying that this Policy is documented, implemented, kept active, disseminated to all staff, and made available to the public.

The process underlying this involvement, in accordance with the standard used in corporate management systems, is divided into the following macro-phases, which are applied in a cyclical sequence according to the PDCA logic

- analysis of processes and identification of related environmental impacts and their measurement through specific indicators;
- assignment of roles and responsibilities, definition of objectives and targets, and allocation of an adequate budget;
- planning, evaluation, and implementation of improvement actions;
- periodic verification of the effectiveness of the actions implemented and reporting on progress towards the achievement of objectives and targets;
- review of the process and possible reworking of the action plan.

Senior management also ensures that all functions involved in the Integrated Management System processes are aware of the applicable requirements and receive adequate training and information regarding the related objectives, roles, and responsibilities.

3.2. Structure responsible for information security management

The structure responsible for the information security management system shall promote, in order to make the general security policy consistent with the evolution of the business context, any actions to be taken in the event of occurrences such as:

- new threats or changes to those considered in previous risk analysis activities;
- significant security incidents;
- changes in the regulatory and legislative context regarding information security;
- results of analyses on the costs, impacts, effectiveness, and efficiency of the information security management system.

3.3. Management and SEC function

Management is the top corporate function responsible, with the support of the main management function, the Information Security Office (CISO), and the structure responsible for the information security management system (ISMS Manager), for top-level decisions regarding security issues.

In particular, it is responsible for supporting and ensuring, through subordinate corporate functions, the application of the general policies of the Information Security Management System, defining appropriate risk management policies, and constantly supporting the process of raising awareness of security issues.

The Information Security function, led by the CISO, supports senior management in implementing the technical and organizational measures necessary for NIS2 compliance, coordinating the risk management process, incident monitoring, and the implementation of the prescribed security measures.

4. CONCLUSIONS

This Integrated Policy constitutes the guidelines that all personnel are required to comply with in the performance of their duties and the framework for planning and managing their activities and reviewing the objectives and targets set.

The principle of continuous improvement ensures that the commitments made in the Integrated Policy are periodically reviewed, updated, and reinforced based on the results achieved, changes in the context, and the expectations of stakeholders.

This document is reviewed annually at the meeting for the preparation of the Management Review.