
	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

<b>Edited by:</b>	Michela Pecchia	Head of HR Organization & Learning Development	<i>F.to Michela Pecchia</i>
<b>Validated by</b>	Lorenzo Lombardi d'Aquino	Chief Human Resource & Organization Officer	<i>F.to Lorenzo Lombardi d'Aquino</i>
<b>Verified by:</b>	Marcello Vispi	Vice President	<i>F.to Marcello Vispi</i>
<b>Approved by:</b>	Renato Brunetti	Chairman & CEO	<i>F.to Renato Brunetti</i>


## Summary

1. INTRODUCTION.....	4
1.1 Background and scope of application of the standard .....	4
1.2 General Objectives of the SGI.....	6
1.3 Operational Objectives for the Reporting Year .....	10
1.2.2 Community and international standardization reference standards .....	11
1.2.3 Relevant national and industry standards .....	12
1.3. Documented Information (Documents) of the QMS.....	12
2 POLICY .....	12
2.1 General Principles of Quality .....	12
2.2 General Principles of Environmental Management Security.....	14
2.2 General Principles of Occupational Health and Safety.....	15
2.2 General Principles of Information Security .....	15
2.2.1 Identification, classification and management of resources .....	16
2.2.2 Secure logical access management.....	16
2.2.3 Behavioral standards for the safe management of corporate resources .....	16
2.2.4 Personnel and security .....	17
2.2.5 Management of abnormal events and incidents.....	17
2.2.6 Physical security management.....	17
2.2.7 Information security management for cloud services.....	18
2.2.8 Contractual aspects related to information security.....	18
2.2.9 Business Continuity Management .....	19
2.2.10 Monitoring, tracking and technical verification .....	19
2.2.11 Life cycle of systems and services.....	19
2.2.12 Compliance with Regulations .....	20
2.2.13 Security of customer data managed through IaaS, PaaS and SaaS services sold.....	20
3 DEFINITION OF ROLES AND RESPONSIBILITIES.....	21
3.0 Responsibility of the environmental management system.....	21
3.1 Structure responsible for information security management .....	22
3.2 Management and SEC Function .....	22
4 Conclusions .....	22

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

## Revision matrix

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

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

## 1. INTRODUCTION

### 1.1 Background and scope of application of the standard

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

These principles, as defined in Section 4.4. of the QM, are embodied in documented information proper to the System (such as the QM itself, Procedures, Operating Instructions, Regulations and in the additional documentation in corporate use - EL7.5.3A) for the purpose of maintaining a Quality Management System (QMS) and Information Security (ISMS) as generically defined in Section 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 above standards.


The aforementioned documented information is to be understood as supplemented by the documented information proper to the Privacy Organizational Model (MOP), applied by the Organization in compliance with the current and applicable regulatory provisions, national and European, regarding 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 but not limited to:
  - Provisions on System Administrators.
  - Provisions on the Processing of Biometric Data.
  - Data Breach Measures.
  - and further

and of which the Data Protection Policy document is an organic expression.

**The scope of the Quality and Environmental Management System** (QM Section 1.3 and 4.3) 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 Telecommunication Networks and Fiber Local Area Networks and Internet of Things operating through various transmission media and different applications (IAF28).*

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

**The scope of the Information Security System** (Section 1.3 and 4.3 of the QM) and, consequently, the related Unidata Policy has been defined as follows:

*Infrastructure Management of the physical and logical security of its Data Center and related Facility Management and delivery 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 June 05, 2020 applicability statement (IAF 33)*

In accordance with the declaration of applicability dated 07.05.2021

For the implementation of the above-mentioned service delivery activities, Unidata makes use not only of its own operational infrastructure at its registered office but also of the infrastructure, understood in the physical and logical sense, called the Unidata Internet Data Centre (hereinafter IDC), also located at Unidata's registered office in:

**Rome, Viale A. G. Eiffel, 100 - 00148 Rome c/o Commercium Mod. M26**

**Milan, Viale Edoardo Jenner 33**

**Modugno (BA), Via delle Dalie 5**


In the aforementioned infrastructure, systems and data processing/management equipment (generically "apparatus/servers") are housed in environments with appropriate infrastructural security measures, both physical and logical/IT, as described below:

- **physical and/or virtual servers owned by Unidata** and directly deputed to the operation of the information systems necessary to ensure the management of the "business mission" ("**vital**" and/or "**Critical**" **business systems**) i.e., the delivery of "information technology, Internet access and additional next-generation" services to the end user (Customer base);
- **physical and/or virtual servers owned by Unidata, entrusted for management to end users/Customers (Hosting)** for the operation of services unrelated to Unidata's competence and responsibility that fall within the scope of Unidata's competence and responsibility in relation to their proper operation in operation and in relation to compliance with the obligations of monitoring, surveillance and support in the repression of crimes provided for by the current national legislation;
- **Customer-owned physical servers hosted (Housing)** at said infrastructure for the operation of services totally outside Unidata's competence and responsibility and totally and directly falling within the remit and responsibility of the entrusted user/Customer;
- **Areas (physical perimeters) under exclusive lease to user/client (Co-location)** with or without access to the facilities referred to in the following section

The aforementioned premises pertaining to the IDC infrastructure, in addition to being equipped with suitable main services of so-called "connectivity" through the presence and availability of diversified "flows" directed to the management of data interchange over networks

*Unidata S.p.A. Internal use - All rights reserved*

Code P5	Issue Date: 23/01/2024	Revision:5	Page5 of 23
---------	------------------------	------------	-------------

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

national/international with access to the Internet Network, also provide the following instrumental services (so-called "facility"):

- access control system
- video surveillance system
- Direct power supply system (primary power supply system) and indirect power supply system (back up power supply systems - UPS and uninterruptible power supply unit)
- Environmental conditioning system and related alarmism
- fire and anti-flooding system
- Computer logical protection systems (firewalling - antivirus - etc.)
- monitoring and alarming systems
- System and/or dedicated technical support system (where contracted)

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

- Internet Access services wired/wireless, fiber optic(NGAN), copper and radio (hiperlan)
- Landline voice telephony services in VoIP technology, remote and virtual switchboard, fax server
- Data center services (Housing, hosting, colocation, cloud, email and more)

For a more comprehensive and detailed description of the infrastructure as a whole and the security measures applied therein, please refer to the following documents:

D7.1A Internet Data Centre

D7.1B - Network Infrastructure

What is subsequently described in this document and in the additional reference documentation for the Quality Management System and the Information Security Management System, must be understood, therefore, as applied to the aforementioned physical-logical perimeter as well as to the processes, resources and/or labor relations (Employees/Collaborators/Third Party assignees) related and/or connected to the due management in operation of the aforementioned infrastructure within the broader and more general corporate purposes.


## 1.2 General Objectives of the SGI

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

**SGI** has as its primary objective the protection of data and the elements of the information system responsible for their management.

Specifically, pursuing information security means defining, achieving and maintaining the following information properties:

- Confidentiality: ensuring that information is accessible only to duly authorized individuals and/or processes;

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

- Integrity: safeguard the consistency of information from unauthorized modification;
- Availability: ensuring that authorized users have access to information and associated architectural elements when they request them;
- Authenticity: ensuring the provenance of information;
- Non-repudiation: ensuring 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 result, in the context of any business activity, in damage to the corporate image, lack of customer satisfaction, 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 to ensure 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 security needs both external and arising from the mandatory. This activity is carried out by drawing on a variety of sources:

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

The results of the assessment help determine what actions are needed to manage the identified risks and the most appropriate security measures with respect to its objectives, based on the definition of the level of residual risk that the company decides to accept, to be implemented later.


To the extent expressed above, this policy, in compliance with the main regulations and standards on the subject:

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

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

- the goal of ensuring complete satisfaction of customer expectations through the provision of quality services that are the result of the standards defined in its Quality Management System.
- the goal 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.

UNIDATA's Quality, Environment and Information Security Policy is divided into the following general objectives:


	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

- To develop and maintain a Quality Management System in accordance with UNI EN ISO 9001:2015 and UNI EN ISO 14001:2015 standards as a means of achieving objectives, meeting commitments, promoting continuous improvement of business processes, and ensuring compliance with mandatory requirements for products and related services;
- To develop and maintain an Information Security Management System that complies with ISO/IEC 27001:2017 and ISO/IEC 27017:2021 and ISO/IEC 27018:2020 as a tool to systematically and continuously control the processes that affect the security of the company's entire information assets, not only from an IT perspective (electronic or paper media used to store documents and data) but especially from a management and organizational perspective by defining roles, responsibilities and formal procedures to ensure the proper operation of the company itself.
- Adopt an integrated risk management system to ensure that for all products/services provided, residual risk is minimized;
- To spread the culture of the environment and eco-sustainable development;
- utmost attention to the special waste produced, ensuring maximum respect for the environment and current regulations;
- Increased environmental awareness among key stakeholders (people inside or outside the enterprise, with different interests and needs, who can influence the choices and behavior of the enterprise and affect its success).
- Engage all available energy and skills in listening to the customer's directions, suggestions, wishes, including through "on field" activity;
- Focus every activity on the customer's needs to satisfy them better and faster so as to establish a leading position in the market;
- To consolidate the relationship with partners in order to ensure higher value, safe, reliable, high-tech products at reasonable prices for customers;
- To provide products and services adhering to all requirements imposed by relevant legislative provisions;
- disseminate appropriate culture and methodologies in the organization so that everyone working there is constantly able to deliver the best expected service to the customer;
- Ensure a high level of satisfaction of all employees through the pursuit of maximum loyalty and sense of responsibility;
- Encourage staff and management so that they can realize their aptitudes, interests and predispositions and develop their technical and organizational skills;

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

- Direct, continuous and permanent commitment to the management of the Quality, Information Security and Environmental Management System;



	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

- Direct, full and informed involvement and participation of company personnel at all levels in the implementation of the Integrated Management System;
- Establishment of close cooperation and transparency with Suppliers to improve the environmental impacts of purchased products/services;
- Commitment to legislative compliance in general and environmental compliance in particular, pollution prevention and continuous improvement

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

Management aware of the importance of environmental protection to its image as well as its responsibilities towards the protection of the surrounding area, has decided to have an Environmental Management System (EMS) such as to enable the reduction of the main environmental impacts and keep the aspects related to its activities under control, thus taking an active role towards the environment.


In addition, Unidata S.p.A. believes that it must assume responsibility within the scope of its operations with reference to at least the following *UN Global Sustainable Development Goals*<sup>1</sup>:

- The need for sustainable investment in the infrastructure required for the deployment of communication technologies;
- The importance of deploying the *smart city* model to make cities inclusive, safe, resilient and sustainable;
- Promote resource and energy use efficiency;
- The need for swift 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 as a corporate priority the preservation of the territory with a commitment to use the necessary resources with the utmost care and with responsible environmental management according to a system aimed at continuous improvement of its performance.

In order to ensure the protection and welfare of its workers, as well as all stakeholders gravitating within its sphere of action and influence, Unidata is committed to:

<sup>1</sup>United Nations General Assembly - New York 26-30/09/ 2015

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

- 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 worker representatives;
- To provide safe and healthy working conditions for the prevention of work-related injuries and illnesses by eliminating hazards and reducing OSH risks as determined by its own context analysis and OSH risk assessments;

### 1.3 Operational Goals for the Reporting Year

The Top Management then on an annual basis provides for the definition and dissemination of a Plan containing the objectives for the reference year that declines in detail the general objectives by involving the relevant levels and the relevant Business Functions within the Organization with the aim of increasing/improving the level of satisfaction of the Customer and the additional Stakeholders.

This document is identified as follows:

P6.2 Plan of Operational Objectives <reference year>


This Quality, Environment and Information Security Policy, c is reviewed and updated at least annually as part of the Senior Management Review (Section 9.3 of the Standard) and/or as needed.

Lack of adequate levels of product/service quality, can result, in the context of any business activity, in damage to the corporate image, lack of customer satisfaction, 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 to ensure 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 relations (employees/collaborators) and in external relations (users/suppliers).

The results of the assessment help determine what actions are needed to manage the identified risks, procedures and measures that are most appropriate with respect to one's objectives.

- **Guiding Principles:** are stated in Chapter 2 of this Policy entitled "Policy." They represent the value system in which the company believes with reference to the quality management of its production/delivery system. They are the basic ideas that the company has developed with regard to quality, i.e., what is right to do, or not to do, in order to have an efficient, effective quality management system that is appropriate to its own and the needs of the market. The primary reference of general safety principles is the standard UNI EN ISO 9001:2015 and UNI EN ISO 14001:2015.
- **Laws and contracts:** within the existing regulatory framework, guidance is provided on how to deal with issues related to maintaining a qualitatively high level of quality in the provision of services to users, in the performance of related work tasks, in relations with suppliers, collaborators, technical and commercial partners . Compliance with Italian legislation relating to the protection and safety in the work environment, the protection of Consumers, fairness in professional and business relationships, as well as the constant pursuit

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

of ethical goals in such areas serves not only to limit the risks of company involvement, but also to ensure an appropriate level of quality of the company's production system.

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

- emphasizes the importance of ensuring Product/Service Quality and the tools to achieve and maintain it;
- is consistent with the company's expressed desire to ensure end-user satisfaction with said products/services;
- is concerned with physical, logical and organizational aspects of the Quality Management System.

Senior management is also committed to:

- **Disseminate and promote** quality policy;
- **Implement** the quality policy by setting improvement goals;
- **Review** the quality policy according to achievements and business strategies.

And to ensure that:


- Information is protected from unauthorized access with respect for confidentiality and is available only to authorized users;
- Information is not disclosed to unauthorized persons as a result of deliberate action or negligence and, in keeping with integrity, is safeguarded from unauthorized modification;
- Plans for business continuity are prepared and that these plans are kept as up-to-date and monitored as possible;
- Staff receive training on information security;
- All breaches of information security and possible weaknesses be reported to those in charge and examined.

Through the implementation of this policy, Unidata intends to fulfill the commitment of compliance with UNI CEI ISO/IEC 27001:2017, UNI EN ISO 9001:2015, 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 goal, 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.

### 1.2.2 Community and international standardization reference standards

- UNI EN ISO 9001:2015 "Quality Management Systems - Requirements "
- ISO 9000:2015 "Fundamentals and vocabulary of quality management systems."

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

- 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"

### 1.2.3 Relevant national and industry standards

- Legislative Decree 206/2005 Consumer Code
- Legislative Decree 259/2003 Electronic Communications Code
- D.Lgs.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 et seq. Consolidated text on the protection of health and safety in the workplace"

### 1.3. Documented Information (Documents) of the QMS


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

## 2 POLICY

### 2.1 General Principles of Quality

The general principles by which Unidata inspires its Quality Policy, in the specific scope of Unidata's IMS referred to in Section 1.1, are articulated as follows:

- Ensure that the requirements of Clients and stakeholders are well defined and a key part of the proposed solutions;
- Ensure that the characteristics of the product or service offered are guided by the principle of maximum disclosure and transparency;
- Ensure clear and constantly improving delivery and maintenance processes;
- Always strive to deliver service to Customers in line with the performance expressed in the Service Charter;
- Ensure at every level of the company conduct that respects the commitments made in the Unidata Code of Ethics;

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

- Always keep in mind that the only reason for Unidata's existence is in the quality of relationships and the quality of services offered to Clients;
- Ensure compliance with current legislation;
- Ensure management system compliance;
- Ensure the adequacy of the facility and equipment.
- Evaluate the impacts of their 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 engaged in their implementation to the best of their ability (process approach);
- Communicating the importance of ensuring the effectiveness and compliance of the QMS to all stakeholders and actively involving, 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 improving the QMS (leadership);
- Evaluate and deal with risks associated with processes and the achievement of its strategic objectives; Exploit and reinforce identified opportunities (risk and opportunity assessment).
- 


**Based on these principles, as part of its QMS, Unidata**

Commits to:

- toward customers, to provide products and services that meet mandatory requirements and are of high quality, to demonstrate transparency and reliability, and to ensure product quality at competitive prices through analysis and cost containment;
- toward suppliers, to foster a fruitful "alliance" so that they can be an active participant in defining product performance and characteristics, and to provide the necessary support in understanding and defining the Customer's requirements and the mandatory requirements relevant to the product;
- toward employees to foster initiative, encourage professional growth, ensure fruitful and peaceful professional relationships, and provide a safe working environment in which everyone can be satisfied;
- toward the Ownership to foster the growth of the Company, ensuring adequate profitability and financial stability, which are indispensable elements for the affirmation of the Quality Policy.

It aims to:

- Develop and maintain a Quality Management System that complies with UNI EN ISO 9001:2015, UNI EN ISO 14001:2015 to ISO IEC 27001:2017 and ISO/IEC 27017:2021 and ISO/IEC 27018:2020, ISO 45001:2018 as a tool to realize goals, meet commitments, promote continuous improvement of business processes, and ensure compliance with mandatory requirements for products and related services;
- Adopt an integrated risk management system to ensure that for all products/services provided, residual risk is minimized;

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

- Engage all available energy and skills in listening to the customer's directions, suggestions, wishes, including through "on field" activity;
- Focus every activity on the customer's needs to satisfy them better and faster so as to establish a leading position in the market;
- To consolidate the relationship with partners in order to ensure higher value, safe, reliable, high-tech products at reasonable prices for customers;
- To provide products and services adhering to all requirements imposed by relevant legislative provisions;
- disseminate appropriate culture and methodologies in the organization so that everyone working there is constantly able to deliver the best expected service to the customer;
- Ensure a high level of satisfaction of all employees through the pursuit of maximum loyalty and sense of responsibility;
- Encourage staff and management so that they can realize their aptitudes, interests and predispositions and develop their technical and organizational skills;
- Communicate and update quality guidelines, commitments and goals annually;
- Convene specific meetings periodically, so that at each level the need to meet requirements under contracts and specifications is known and shared, and to make updates required by evolving mandatory standards;
- Ensure that the objectives of the quality policy are defined and compatible with the context and strategic direction of the company and include information security;
- Ensure the integration of integrated management system requirements into corporate business processes.
- Communicate the Company Policy with all employees.

**Blinds to:**

- Develop service techniques designed and implemented to meet customer needs, anticipate customer expectations, and provide solutions that create value for the customer;
- To operate a systematic selection of 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, using all the necessary potential.


**Unidata's work complies with the following principles:**

- Collaboration with certification bodies;
- Collaboration with clients.

## 2.2 General Principles of Environmental Management Safety

The general principles by which Unidata inspires its Environmental Policy, in the specific scope of Unidata's IMS mentioned in Section 1.1, are articulated as follows:

- Implement all possible pollution prevention actions, 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;

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

- Raise employee awareness through appropriate information and training programs so that personnel at all levels ensure the effective implementation of the Environmental Management System within the scope of their responsibilities by adopting green-office behavior;
- Promote and disseminate "environmental" culture to all stakeholders including customers, partners, suppliers, etc;
- Take into account in the qualification and evaluation process of suppliers environmental performance criteria;
- Promote "Smart Working" by fostering the sustainable mobility of employees and contractors;
- Prioritize sustainable and/or eco-friendly purchases;
- Promote recycling and recovery;

## 2.2 General Principles of Occupational Health and Safety


The general principles by which Unidata inspires its Occupational Health and Safety Policy, in the specific scope of Unidata's IMS referred to in Section 1.1, are articulated as follows:

- monitor the Company's application and compliance with OSH standards to its stakeholders through specific control methods and tools;
- Promote the involvement and participation of workers and especially worker representatives in the process of risk assessment and mitigation of OSH hazards;
- Raise employee awareness through appropriate information and training programs so that personnel at all levels ensure the effective implementation of the OSH Management System within their responsibilities and succeed in monitoring near misses in order to prevent occupational injuries, accidents and illnesses;
- Ensure involvement and discussion between the relevant figures of the two Management Systems: Corporate Social Responsibility and OSH;

## 2.2 General Principles of Information Security

The general principles by which Unidata inspires its **Information Security Management Policy**, in the specific scope of application of the standard mentioned in Section 1.1, are articulated in the following themes:

- Identification, classification and management of resources
- Secure logical access management
- Behavioral standards for the safe management of corporate resources
- Personnel and Security
- Management of abnormal events and incidents
- Physical security management

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

- Contractual aspects related to information security
- Business Continuity Management
- Monitoring, tracking and technical verification
- Life cycle of systems and services
- Compliance with regulations

Below is the objective and guidelines defined by Unidata for each topic.

### 2.2.1 Identification, classification and management of resources

**Goal:** *All Unidata staff and, when relevant, contractors, should receive appropriate awareness, education, training and coaching, and periodic updates on organizational policies and procedures, in a manner relevant to their work*

- ☐ A census system of all tangible and intangible assets to be protected (information, hardware, software, paper records and storage media) must exist and be kept up-to-date over time;
- ☐ Each resource (tangible/intangible asset) must be directly assignable to a responsible Business Function.
- ☐ Information should be classified according to its level of criticality so that it is managed with consistent and appropriate levels of confidentiality and integrity. The criticality of information must be assessed as objectively as possible through the use of appropriate working methodologies.
- ☐ Management methods and protection systems for information and the assets on which it resides must be consistent with the level of criticality identified.

**Points of the Norm:**

7.2, Annex A - ISO/IEC 27001:2017.

### 2.2.2 Secure logical access management

**Goal:** *ensure secure access to information, so as to prevent unauthorized processing of information or its viewing by users who do not have the necessary rights.*

- ☐ Each individual user's access to information must be limited to only the information he or she needs to perform his or her duties (so-called "need-to-know" principle). 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 conditional on passing a procedure to identify and authenticate them.
- ☐ Information access authorizations should be differentiated according to the role and positions held by individuals and should be reviewed periodically.
- ☐ A process for managing authorization credentials and related access profiles must be defined.
- ☐ The systems that constitute the ICT infrastructure must be properly protected and segregated so as to minimize the possibility of unauthorized access.


**Points of the Norm:**

11, Annex A - ISO/IEC 27001:2017

### 2.2.3 Behavioral standards for the safe management of corporate resources

**Goal:** *ensure that Unidata's employees and contractors adopt behavior patterns designed to ensure adequate levels of information security.*



	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

- ☐ Work environments and corporate resources must be used in a manner congruent with the purposes for which they were made available and ensuring the security of the information processed.
- ☐ Procedures must be established for the management and use of information in both digital and paper media.
- ☐ Company computer systems must be used by employees and contractors according to approved procedures.

#### National regulations:

General Data Protection Regulation (EU Regulation 2016/679 - GDPR) Legislative Decree 101/2018 (National Adaptation to the European Privacy Regulation) [Points of the Rule:](#) 8.2 and 11.1, Annex A - ISO/IEC 27001:2017

### 2.2.4 Personnel and security

**Goal:** *To ensure that personnel working on behalf of Unidata (employees and contractors), have full awareness of information security issues.*

- ☐ In the selection and induction phases of personnel into Unidata, levels of knowledge of the company's security objectives and issues must be assessed according to the activities to be performed.
- ☐ While at Unidata, personnel must receive adequate and ongoing training inherent in data security issues.
- ☐ The manner of termination of employment with Unidata should be consistent with corporate security objectives.

#### Points of the Norm:

7.2, Annex A -ISO/IEC 27001:2017

### 2.2.5 Management of abnormal events and incidents

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

- ☐ All employees and contractors are required to detect and notify, to those in charge and according to appropriate procedures, any information security issues.
- ☐ Incidents that may impact security levels should be detected and any damage, potential or otherwise, should be handled promptly where possible according to specific procedures.
- ☐ There must be a system for recording and classifying incidents and abnormal events in order to carry out analyses to improve safety levels consistent with the actual problems encountered.


#### Points of the Norm:

16, Annex A - ISO/IEC 27001:2017

### 2.2.6 Physical security management

**Goal:** *prevent unauthorized access to corporate offices and individual business premises and ensure adequate levels of security for the areas and assets through which information is managed.*

- ☐ **Security management of areas and premises through must be ensured:**
  - The identification of areas and classification of premises according to the criticality of the processed information;
  - The definition of appropriate levels of protection;
  - The preparation of a periodic cycle of checks and controls.

 <b>UNIDATA</b>	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

- ☐ **Equipment security must be ensured through:**
- The definition of appropriate location of information processing equipment;
  - The provision of resources necessary for their operation;
  - The provision of an appropriate level of maintenance;
  - The preparation of a periodic cycle of checks and controls.

[Points of the Norm:](#)

11.1, Annex A -ISO/IEC 27001:2017

### 2.2.7 Information security management for cloud services

<u>Cloud service client</u>	<u>Cloud service provider (Unidata)</u>
<p>The cloud service customer is properly informed for everything related to the following:</p> <ul style="list-style-type: none"> <li>- Information stored in cloud computing environment can be accessed and managed by Unidata;</li> <li>- Resources can be maintained in the cloud computing environment, for example, application programs;</li> <li>- Cloud service administrators have privileged access.</li> </ul>	<p>Unidata provides guarantees in the following areas:</p> <ul style="list-style-type: none"> <li>- Basic information security requirements applicable to cloud service design and implementation</li> <li>- Authorised insider hazards</li> <li>- Access to customers' cloud services activities by Unidata staff.</li> <li>- Assurance regarding access control procedures</li> <li>- Ready communications during change management</li> <li>- The guarantee of data protection</li> <li>- Customer <i>account</i> lifecycle management</li> <li>- Breach reporting and information sharing guidelines to support forensic investigation and analysis</li> </ul>

### 2.2.8 Contractual aspects related to information security


**Goal:** *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 Unidata has to establish with those third parties.*

- ☐ Agreements with third parties and outsourcers that 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 for the protection of personal data ("privacy regulations").

[National regulations:](#)

General Data Protection Regulation (EU Regulation 2016/679 - GDPR) Legislative Decree 101/2018 (National Adaptation to the European Privacy Regulation) [Points of the Rule:](#)

6.1, 15 and 18.1, Annex A -ISO/IEC 27001:2017

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

### 2.2.9 Business Continuity Management

**Goal:** *To ensure the continuity of Unidata's business and the eventual timely restoration of services provided affected by abnormal events of a certain severity, reducing the consequences both inside and outside the business environment.*

- All events on which a disruption of business continuity may depend must be carefully identified and evaluated in terms of probability of occurrence and possible consequences.
- A continuity plan must be in place that enables the organization to deal, in an organized and efficient manner, with the consequences of an unforeseen event by ensuring the restoration of critical services in a timeframe and manner that allows for the reduction of negative consequences to the business mission.
- All necessary operational and organizational procedures 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.
- Maintenance and updating of the plans and procedures in the above points must be ensured in order to ensure the effectiveness of the system over time in the face of any organizational/technological changes.

[Points of the Norm:](#)

17.1, Annex A - ISO/IEC 27001:2017

### 2.2.10 Monitoring, tracking and technical verification

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

- ☐ Information systems must be periodically checked so as to assess the proper functioning of the security systems, hardware and software, implemented, as well as the possible presence of vulnerabilities not found or known in the past.
- ☐ Periodic analysis activities should be carried out against the results of all monitoring, tracking and verification activities, aimed at identifying critical areas and appropriate corrective and improvement actions.
- ☐ Periodic audit activities of the information security management system must be planned. [Points of the](#)


[Standard:](#)

16.1, Annex A - ISO/IEC 27001:2017

### 2.2.11 Life cycle of systems and services

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

- ☐ Security aspects must be appropriately considered in 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 test environments with use of formal acceptance procedures when switching between environments.
- ☐ Safety aspects must be appropriately considered in the operation phase. In particular, the following issues must be addressed:
  - Capacity management of the technology infrastructure;

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

- Securitization of systems and data (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 erasure of disks);
- Network security: network segregation, gateway monitoring (firewall).

- ☐ Safety aspects must be appropriately considered in the management of services. In particular, the following issues must be addressed:
- Monitoring of systems and services;
  - utilities management;
  - performance monitoring.

#### Points of the Norm:

12, Annex A - ISO/IEC 27001:2017

### 2.2.12 Compliance with Regulations

**Goal:** *To ensure compliance with the provisions of the law, statutes, regulations or contractual obligations and any requirements inherent in information security, while minimizing the risk of legal or administrative sanctions, significant loss or reputational damage.*

- All regulatory and contractual requirements regarding information system security and impacting the Information Security Management System must be identified and analyzed in order to assess their impacts on the organization and information systems.
- Managers in the various areas must ensure, each within their area of responsibility, that all policies, procedures, standards, and generally all documentation related to information security are implemented and adhered to.
- Failure to comply with the provisions of this document, and all others that flow from it, will be handled in accordance with the provisions of the CCNL or, in the case of third-party default, according to existing contractual relationships.


#### Points of the Norm:

15, Annex A -ISO/IEC 27001:2017

### 2.2.13 Security of customer data managed through IaaS, PaaS and SaaS services sold

The company has always made information security and safeguarding a flagship of its systems.

In addition to all systems of data protection from external attacks, backup of the same and state-of-the-art disaster recovery systems, Unidata has decided to adopt, in order to protect the access information of its users, an organic system of security measures, management procedures as well as a documentary system suitable and compliant with national and European requirements on the processing of personal data (Data Protection Policy - General and Particular Security Measures) and the requirements of voluntary certification standards (ISO/IEC 27001; ISO/IEC 27017 and ISO/IEC27018) as a synergistic integration, calibrated to the nature of the services provided to Clients, to the management systems already in place.

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

## 3 DEFINITION OF ROLES AND RESPONSIBILITIES

### 3.0 Responsibility for the environmental management system

Management takes responsibility for establishing and disseminating the Environment Policy within and outside the Company by ensuring that it is:

- *documented, understood, supported, implemented and disseminated to all staff;*
- *Available to anyone who requests it.*

It is the responsibility of management to take timely action on environmental management problems that cannot be solved independently by the appropriate organizational structures.

UNIDATA SPA performs a constant analysis of 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 objectives and targets that can be measured through the use of indicators and a monitoring program of the same that can 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 prevention or mitigation of the most significant aspects that have emerged.

Management is personally involved in the adherence to and implementation of these principles by ensuring and periodically verifying that this Policy is documented, implemented, kept active, disseminated to all personnel, and made available to the public.

The process underlying this involvement, in accordance with the standard in use in business management systems, consists of the following macro-steps that are applied in a cyclic sequence according to a so-called PDCA<sup>2</sup>logic


- Process analysis and identification of related environmental impacts and their measurement through specific indicators;
- Assigning roles and responsibilities and setting goals and objectives and allocating an appropriate budget;
- Planning, enhancement and implementation of improvement actions;
- verification periodic of the effectiveness of the actions put in field  
e reporting of progress toward achieving goals and objectives;
- Review of the process and possible reshaping of the action plan.

<sup>2</sup>The construction of a management system, in general, goes through four stages, viz: Plan = planning (which includes policy and program definition);

Do = implementation (which includes establishing system procedures); Check=

verification (which includes monitoring, records and audits);

Act= action (the actions with which to take action to make changes and improvements and are decided by management review of the system).

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

### 3.1 Structure responsible for information security management

In order to make the overall security policy consistent with the changing business environment, the structure responsible for the information security management system should advocate for possible actions to be taken in the face of the occurrence of events such as:

- ☐ New threats or changes to those considered in previous risk analysis activities;
- ☐ significant security incidents;
- ☐ Evolution of the regulatory and legislative environment for information security;
- ☐ results of analysis on costs, impacts, effectiveness and efficiency of information security management system.

#### National regulations:

DOC RFC\_2350 V.1.6 25/02/2015

Art. 16bis c4 Legislative Decree

no. 70/2012 DPCM 24/01/2013

DPCM 158/2013

Measure on Data Breach Event Management Privacy Guarantor

#### Points of the Rule:

6.1e 18, Annex A -ISO/IEC 27001:2017

### 3.2 Management and SEC Function

Management (Direction) is the apex corporate function that is responsible, with the support of the main SEC (Security) management function and the structure responsible for the information security management system (Resp. SGSI), for making top-level decisions regarding security issues.

In particular, it is responsible for supporting and ensuring, through subordinate business functions, the implementation of the general policies of the Information Security Management System, establishing suitable risk management policies, and continuously supporting the process of raising awareness of security issues.


#### Points of the Norm:

Ch. 5 and 7 ISO/IEC 27001:2017

5.1, Annex A -ISO/IEC 27001:2017

## 4 Conclusions

This Quality, Environmental and Information Security, Occupational Health and Safety Management System Policy constitutes in this regard, the direction to which all personnel are required to conform in the performance of their duties and the framework for the planning and management of their activities and the review of established objectives and targets.

	<b>POLITICS</b>
	Quality, Environment , Information Security, Occupational Health and Safety Policy

The Organization conducts periodic internal audits directed at assessing the effectiveness and adequacy of its IMS. The results of these audits are reviewed by management to identify and plan actions and interventions to enable continuous performance improvement.

This document is reviewed annually at the meeting to prepare the Management Review.