SDP-ITA-PO 01-INTEGRATED MANAGEMENT SYSTEM POLICY

SDP-ITA-PO 01-Integrated Management System Policy

Rev. 8 – 08/02/2025

IMPORTANT: The only official version of this document and the other documents of the Dedalus Integrated Management System including the required forms can be found in the " Sistema Qualità Integrato " archive of the company's SharePoint in Office 365 which is always accessible from the link https://dedalusspa.sharepoint.com/sites/quality, and to which we must always refer to consult the document and download the forms.

Any other source is not official and therefore not reliable.

TABLE OF CONTENTS

1 GENERAL ELEMENTS ON THE INTEGRATED MANAGEMENT SYSTEM POLICY

1.1 Objectives of Dedalus

The goal of Dedalus is to consolidate its role as a leader in the global Health Care Systems market.

1.2 Contents and parts of the Integrated Management System Policy of Dedalus Group

To reach this goal, Top Management of Dedalus Group has defined this **Integrated Management System Policy** for the whole organization.

The policy **contains the strategic elements** that are the keys to maintain an effective and efficient:

1. Quality Management System (**QMS**) built on **ISO 9001** standard
2. Service Management System (**SMS**), built on **ISO/IEC 20000-1** standard
3. Information Security Management System (**ISMS**), built on **ISO/IEC 27001** and its extensions **ISO/IEC 27017** and **ISO/IEC 27018**, defined in document SDP-ITA-PO 03-Information Security and Data Privacy General Policy
4. Environmental Management System (**EMS**), built on **ISO 14001** standard
5. Quality Management System for Medical Devices (**MDQMS**) built on **ISO 13485** standard
6. Social Accountability Management System (**SGRS**), in compliance with the **SA 8000** standard
7. Gender Equality Management System (**GEMS**), in compliance with **UNI PRD 125** practice
8. Business Continuity Management System (**BCMS**), in compliance with the **ISO 22301** standard.

Furthermore, with reference to the Management System for the Prevention of Corruption, in order to comply with the **ISO 37001** standard, the Dedalus Group Anti-Corruption Policy was adopted, approved on 22 December 2022 by the Board of Directors of Dedalus S.p.A., to which reference should be made.

1.3 Parts of the Integrated Management System Policy of Dedalus

Top Management of Dedalus Group ensures that this policy:

- is **appropriate to the purpose and context of the organization** and supports its strategic goals;
- provides a **framework for** setting **goals** for all applicable management systems;
- includes a **commitment to meet the applicable requirements** of all management systems, including mandatory and contractual requirements, and to continually **improve the management systems and** their **effectiveness**;
- includes the organisation's **commitment** to comply with the international documents as listed in section II of SA 8000 on **Normative Elements** and their Interpretation;
- includes a commitment to **comply with national laws**, other applicable laws and other requirements to which it subscribes;
- includes a **commitment to gender equality;**
- is **available** as documented information;
- is **communicated, understood, and applied** within the organization;
- is made available to relevant stakeholders;
- is **reviewed** periodically for continued suitability.

2 POLICY FOR OVERALL QUALITY, SERVICE MANAGEMENT AND MEDICAL DEVICE MANAGEMENT

2.1 Standards applicable to the section

This section of the IMS policy refers specifically to the requirements of **ISO 9001, ISO/IEC 20000-1**, and **ISO 13485**.

2.2 Applicable principles

Top Management strongly believes that the adoption of an IMS results in great benefits in terms of value for our customer and of internal organization improvements, and it has defined the Quality Policy of Dedalus Group, that is built on these **principles**:

- Guarantee and constantly improve **customer satisfaction**, meeting their expectations and complying with **product and service requirements** in order to become a reliable and strategic partner for them;
- Ensure that **customers receive real value through** the delivery of Dedalus Group **services** and the adherence to defined Service Level Agreements;
- Develop **continuous improvement in the quality of our products, services**, and in the Quality System **effectiveness;**

- **Promptly respond to market** developments through a flexible, highly competent and worldwide competitive organization;
- Achieve and constantly maintain the **compliance of** our **medical devices with all the regulatory requirements** of the markets where we sell;
- **Involve the** entire **staff** in processes, supporting them to constantly **grow on their skills** and encouraging them to feel and act as a fundamental part for the quality system and for the continuous improvement of the organization, its products and services.

2.3 What to do to put these principles in practice

The implementation of this policy involved the activation of the following **actions**:

- defining and specifying the **responsibilities, roles, tasks** for the different phases of the processes;
- developing **internal rules** that have been taken on as organizational, procedural and operational reference standards in the management of activities;
- **prevent** the occurrence of **non-conformities** during the performance of processes;
- identify and record non-conformities, promoting the activation of appropriate **corrective actions** and the consolidation of the solutions adopted;
- Promote the **development** of the **skills of professional resources**, promoting integration and collaboration between internal organizational areas and activating permanent training actions;
- enhance the **value of the know-how** possessed, activating the dissemination of good practices and pursuing their optimization in order to make common heritage, working methods and acquired experiences;
- ensure the promotion of the **focus on the customer** throughout the organization, as well as the integrity of the management system itself.

Dedalus Top Management has established appropriate **internal communication** processes such as, for example, through the company website, e-mail, newsletters, video conferences, physical and virtual meetings/meetings between work groups, tools and instruments for sharing information with the utmost respect for the security of such information.

For **external communication** the following tools are basically used: advertising, production of brochures and informative documentation about the organization, websites, organization of events, press office activities, participation in events, knowledge sharing portals, company areas specifically dedicated to experimentation and involvement of customers and stakeholders in knowledge development processes.

3 INFORMATION SECURITY MANAGEMENT POLICY EXTENDED TO CLOUD COMPUTING

The information security policy is defined in SDP-ITA-PO 03-Information Security and Data Privacy General Policy, which is annexed to this document but has its own separate approval cycle.

4 ENVIRONMENTAL POLICY

4.1 Standards applicable to the section

This is the part of the IMS policy which is specifically referred to EMS and to the requirements of **ISO 14001** standard.

4.2 Applicable principles

The environmental impacts of the work processes and activities of Dedalus Group are very low, as we area a service company; however, the company's management believes it is very important that the **organization's activities** are performed with a focus on protecting and **respecting the environment, preventing pollution and minimizing the environmental impacts due to energy consumption and carbon footprint**, as well as **the importance of commitment to green design of ICT infrastructures.**.

To this end, the IMS has also been developed to ensure the continuous reduction of the impact on the environment that the organization's activities may have, in accordance with the requirements of ISO 14001.

The general **goals** of our EMS are:

- Ensure **compliance with** and continued **adherence to applicable legislative** and contractual **requirements** that impact the **environment**;
- **Continuously improve the environmental performances** of the organization's processes in terms of reducing their impact on the environment, lowering the energy consumption, reducing Dedalus carbon footprint, commit to green design of ICT infrastructures, as well as preventing and minimization the pollution directly or indirectly associated to the organization processes.

These general objectives are then detailed from year to year through specific targets, which may include, for example, the following: reducing impacts related to travel for business activities, increasing environmental sustainability in offices and encouraging sustainable purchasing, reuse and recycling, and finally promoting a reduction in the amount of emails sent.

4.3 What to do to put these principles in practice

These objectives become concrete through formal **plans** to reduce environmental impacts, **environmental targets** fixed in accordance to them and **periodical checks** on their achievement.

The EMS is first of all targeted on the own organization of Dedalus Group, where the actions taken can have the highest impact, but as far as possible Dedalus Group aims also to promote consistent and environmentally conscious behaviour **of all its suppliers, customers and stakeholders** in general.

5 SOCIAL RESPONSIBILITY POLICY

5.1 Standards applicable to the section

The part of the Quality Management System that concerns Social Responsibility is the SGRS (Social Responsibility Management System); the reference standard for this system is **SA8000**.

5.2 Applicable principles

The Management gives all areas the mandate to continuously and systematically improve health and safety performance, risk reduction and the defence of human and labour rights. The Management undertakes not to supply or realise products/services if work activities cannot be carried out in complete safety for personnel and the environment and for people's rights and dignity. The Management also aims to increase the company's potential in terms of employment and growth.

In particular, the applicable principles are as follows:

- Promotion of the involvement and conscious participation of the organisation's Personnel at all levels in the implementation of the Integrated Management System, also involving subcontractors who work permanently with the organisation;
- Commitment to constant updating and compliance with the legislation in force and all other prescriptions subscribed to by the organisation including the SA8000 standard and the norms and laws referred to therein;

- Attention to resources and awareness of the importance of their role in the company dynamic, which attributes a pre-eminent role to the training and development of all personnel;
- Continuous and constant research that moves and projects the company workforce towards cutting-edge solutions and technologies that respect health and safety and have a low environmental impact;
- Continuous joint participation of workers and management in the protection of human rights to identify and correct non-conformities and ensure compliance is maintained;
- Constant commitment to comply with all the requirements of the standard for Social Responsibility and compliance with appropriate international instruments (ILO-UN etc.);
- Commitment not to employ, in its workforce, personnel that may fall within the definition of "child" or "young worker" and/or prohibition to support other realities that use or favour child labour;
- Promotion of dialogue and confrontation with all internal and external stakeholders (public authorities, citizens, associations, etc.), taking into account their instances, needs and expectations by activating appropriate tools for participation and communicating the performance of company activities in a transparent manner.

To this end, the Integrated Management System was also developed to guarantee the continuous improvement of processes and activities of the social responsibility system, in compliance with the requirements of the SA8000 standard.

The general objectives of the IMS are

- to ensure compliance and **continuous observance of the applicable legislative and contractual requirements** that have an impact **on social responsibility**;
- to **continuously improve the organisation's processes** in relation to their impact on social responsibility.

These general objectives are then detailed year by year through specific objectives, which may include, for example, the following: improving gender equality, fostering the internal training of people, improving the organisation's social commitment, disseminating the principles of social responsibility along its supply chain.

5.3 Actions developed

These objectives are made concrete through the **planning of activities to improve the responsibility system**, the achievement of which is periodically verified.

6 GENERAL AND SPECIFIC GENDER EQUALITY POLICIES

6.1 Standards applicable to the section

The part of the Integrated Management System that concerns Gender Equality is the GEMS (Gender Equality Management System); the reference standard for this system is the **UNI/PDR 125** practice.

6.2 General gender equality policy

The Management of Dedalus, **in coordination with the Gender Equality Steering Committee (Comitato Guida per la Parità di Genere)** and in accordance with the DNA value of the Dedalus Group, has established this general gender equality policy.
The person responsible for coordinating the implementation of this gender equality policy is the Director of Human Resources for Dedalus Italia, in alignment with the Group's D&I strategy.

This policy stipulates that:

- At Dedalus, **innovation begins with inclusion**. As a company, we are guided by **our core values** and know that diversity and inclusion are **key factors in our success and growth.**
- Our international presence brings together people from all over the world, so we strive to **value diverse backgrounds, skills and experiences** and create **an environment that reflects the many communities we reach.**
- "Pursuing diversity and inclusion" is one of our core values and a part of our Dedalus DNA, which drives us to create a **respectful, diverse and inclusive environment** that recognises **the unique needs**, **perspectives and potential** of all members of our community. Dedalus is proud to promote diversity, inclusion, fairness and equality, and is committed to creating a safe and **inclusive culture where diversity in all its forms is valued and everyone is encouraged** to be the best they can be.
- Dedalus values the diversity that exists in the roles that operate within the organisation and maintains processes capable of developing the empowerment of all personnel, including those of the numerically less represented sex, in business activities.

The main principles are:

- Each of us leads with respect, by example and by being a role model to colleagues, managers, leaders, suppliers, customers and others.
- By embracing difference, eliminating prejudice and challenging negative behaviour, we can be part of a culture where we all feel a sense of belonging.

- Through the diversity of our backgrounds, experiences, opinions or beliefs, together we build a sustainable business.

In order to promote and ensure the achievement and maintenance of this objective, Dedalus focuses its efforts on the following 6 areas of action, as defined by UNI/PDR 125:

1. Culture and strategy
2. Governance
3. Human resources processes
4. Opportunities
5. Compensation Equity
6. Parenting

Dedalus intends to ensure gender equality by means of concrete actions that, in addition to meeting the requirements/KPIs established in each of the areas mentioned, are of real and concrete value to the women present in the organisation, who are the real stakeholders.

The organisation, wishing to pay attention to this satisfaction at all times and in all circumstances of a woman's working life in the organisation, has chosen to manage all the this "life cycle" through the following aspects:

- Selection and recruitment
- Career management
- Pay equity
- Parenting, care
- Work-life balance
- Abuse and harassment prevention

For each of the following aspects, Dedalus Italia has established more specific policies, which are set out below. To each policy expressing the principles by which Dedalus Italia is inspired, the organisation has associated specific and measurable equality objectives indicated in the strategic plan.

6.3 Specific gender equality policies

Dedalus Italia, through the analysis of its business processes, has understood and defined the principles to be respected in relation to each of the following points. These principles are the criteria that inspire the processes to be implemented:

- the existing gaps in relation to the indicators established by the UNI/PDR 125 practice

- the needs of women in the organisation, considered as the main stakeholders in the concrete results of the organisational model

6.3.1 Selection and recruitment policy

Dedalus Italia respects the following principles in the process of selection and recruitment of personnel to be employed in its business activities, with a view to improvement:

- The selection of candidates must be gender neutral.
- Selection criteria must take account of requirements relating to personal qualities such as professionalism, competence, specialisation and experience.
- Selection must not include issues of marriage, pregnancy and family responsibilities.
- Selection must take into account the need for a balanced representation of women and men in the workforce in relation to the total number of people present.
- Top management and budget-delegated roles must be distributed in a gender-balanced manner.
- The position envisaged at the time of recruitment must include a salary that is commensurate with the tasks and responsibilities and not influenced by gender.
- Selection must take into account that the percentages of women and men whose contracts provide for variable remuneration are balanced

6.3.2 Career management policy

Dedalus is aware that the economic results achieved also depend on the people who work there, and all career development opportunities are intended to relate solely to the results and merits of the person, regardless of gender. Dedalus manages the careers of its employees with a view to improvement and in accordance with the following principles:

- The allocation of roles and tasks must take into account the gender balance of management.
- The design and presentation of career paths must be gender inclusive.
- Employee career paths are accessible to all persons who can transparently verify that gender balance is being maintained.

- The working environment, where most of the day is spent, must provide opportunities (technological and physical) for all people to express themselves and to feel safe and comfortable.
- Skills and awareness training is a fundamental process aimed at removing any career barriers and restoring any gender balance in management.
- When staff leave the organisation in the event of redundancy, they are closely scrutinised by reviewing gender attrition.
- Promotions always take into account gender balance at the functional level.
- Ensure that there is a gender balance among panel speakers at roundtables, events, conferences or other events, including scientific ones.

6.3.3 Wage equity policy

Dedalus aims to ensure equal pay for men and women during recruitment and throughout the careers of its employees. The organisation does not asymmetrically take into account the costs of remunerating people of different genders. In determining, paying and adjusting remuneration, the organisation shall respect the following principles:

- People's remuneration shall be recognised in relation to their role and responsibilities, and any additions to this remuneration in the form of benefits and bonuses shall be understood to be based solely on the results achieved and recognised.
- Salaries, bonuses and the allocation of benefits are documented and accessible to all employees in the interests of transparency
- Remuneration, bonus and benefits criteria are documented and accessible to the entire staff
- Any member of staff has the right to report any inequalities

6.3.4 Parenting and care policy

Dedalus does not want to be an obstacle to parenthood and supports motherhood and fatherhood through activities designed to meet the needs of those who, due to their parental status, have to balance their commitment between work and new emerging needs. The organisation supports this intention in the light of the following principles

- Motherhood and parenthood are supported through training, information and reintegration programmes.
- Support maternity before, during and after childbirth

- Paternity leave is promoted so that all potential beneficiaries can benefit from it for the full statutory period.
- Support the return from leave through specific reintegration initiatives
- Dedalus plays an active role in supporting the activities of caregivers (care of the unborn child) with concrete initiatives.

6.3.5 Work-life balance policy

Dedalus wants to offer its employees the opportunity to manage the time they devote to life and work by striking a balance that takes into account both the company's objectives and the employee's psycho-physical well-being, which results from greater freedom of self-determination. The principles of work-life balance are as follows:

- Work-life balance measures are aimed at all employees, regardless of gender.
- Dedalus adopts part-time working for roles where possible, flexible working hours and smart working.
- Dedalus allows telematic connection with all employees working externally (regardless of contract) for work processes and participation in meetings.

6.3.6 Abuse and Harassment Prevention Policy

Dedalus rejects all forms of abuse and harassment and therefore has a **zero-tolerance** policy for the prevention and repression of this phenomenon. Dedalus implements its prevention policy through concrete actions, the principles of which include:

- Identifying the risks of abuse and harassment
- That Dedalus plans preventive actions in relation to this risk
- The possibility of reporting suspicions and/or facts relating to abuse and harassment through the company's whistleblowing procedure.
- Dedalus' absolute protection of whistleblowers from possible subsequent retaliation.
- That Dedalus analyses and understands all incidents of abuse and harassment
- The development of courteous and gender neutral communication
- Dedalus' absolute protection of reporters from any subsequent retaliation
- That Dedalus analyses and understands all incidents of abuse and harassment
- The development of courteous and gender neutral communication

6.4 Actions developed

These objectives are made concrete through **the planning of activities to improve the gender equality management system**, the achievement and updating of which is periodically verified.

7 BUSINESS CONTINUITY POLICY

7.1 Standards applicable to the section

The part of the Integrated Management System that concerns Business Continuity is the Business Continuity Management System; the reference standard for this system is **ISO 22301**.

7.2 Applicable Principles

In accordance with the reference standard ISO 22301 (in its latest version), Dedalus Italia's management is actively involved and committed to promoting the actions and activities for planning, implementing, verifying, maintaining and improving the Business Continuity Management System (BCMS) as a component of the Integrated Management System.
The Dedalus BCMS aims to facilitate the achievement of business objectives, in the face of disruptive events that could compromise the delivery of products and services.
In fact, the company's management believes that the operational continuity of the company's processes is fundamental in order to guarantee the fulfilment of all the commitments made by the organisation to customers and stakeholders and, in general, to ensure the survival of the organisation itself in the event of disasters or other extraordinary events that could jeopardise its normal operations.
Management is committed to meeting all applicable business continuity requirements through the implementation and continuous improvement of the Business Continuity Management System.

The general objectives of the BCMS are:

- ensuring **compliance with the continuity commitments of the services provided, including services provided in SaaS**, made by the organisation to customers and stakeholders;
- prevent, as far as possible, “critical” situations for **business continuity**;
- mitigate the **negative impacts** on the business as a result of the possible occurrence of "critical" business continuity situations;
- ensure the survival of the **organisation itself in the event of disasters or other extraordinary events** that could endanger the normal operation of the organisation;
- increase the **trust of customers and stakeholders** in Dedalus Italia and the services it provides.

These general objectives are then detailed year by year through specific objectives.

7.3 Actions developed

These objectives are given concrete form through the activities envisaged by the BCMS, and in particular through:

- the periodic development of **Business Impact Analysis** (**BIA**) to identify critical services and processes, including SaaS services;
- the performance of **Risk Analyses**, to assess the unavailability scenarios arising from the events that make up the corporate risk landscape;
- the development of **Business Continuity Plans**, including for SaaS services;
- the scheduled **testing** of these Business Continuity Plans and the adoption of appropriate **countermeasures and improvements** for any aspects to be optimised;
- the execution of **training campaigns** aimed at raising the awareness of the corporate population and spreading **knowledge** on the subject of Business Continuity.

8 OUR CORE VALUES

We strongly believe that in order to achieve real quality at 360 degrees, each of us must adopt the following principles on a daily basis:

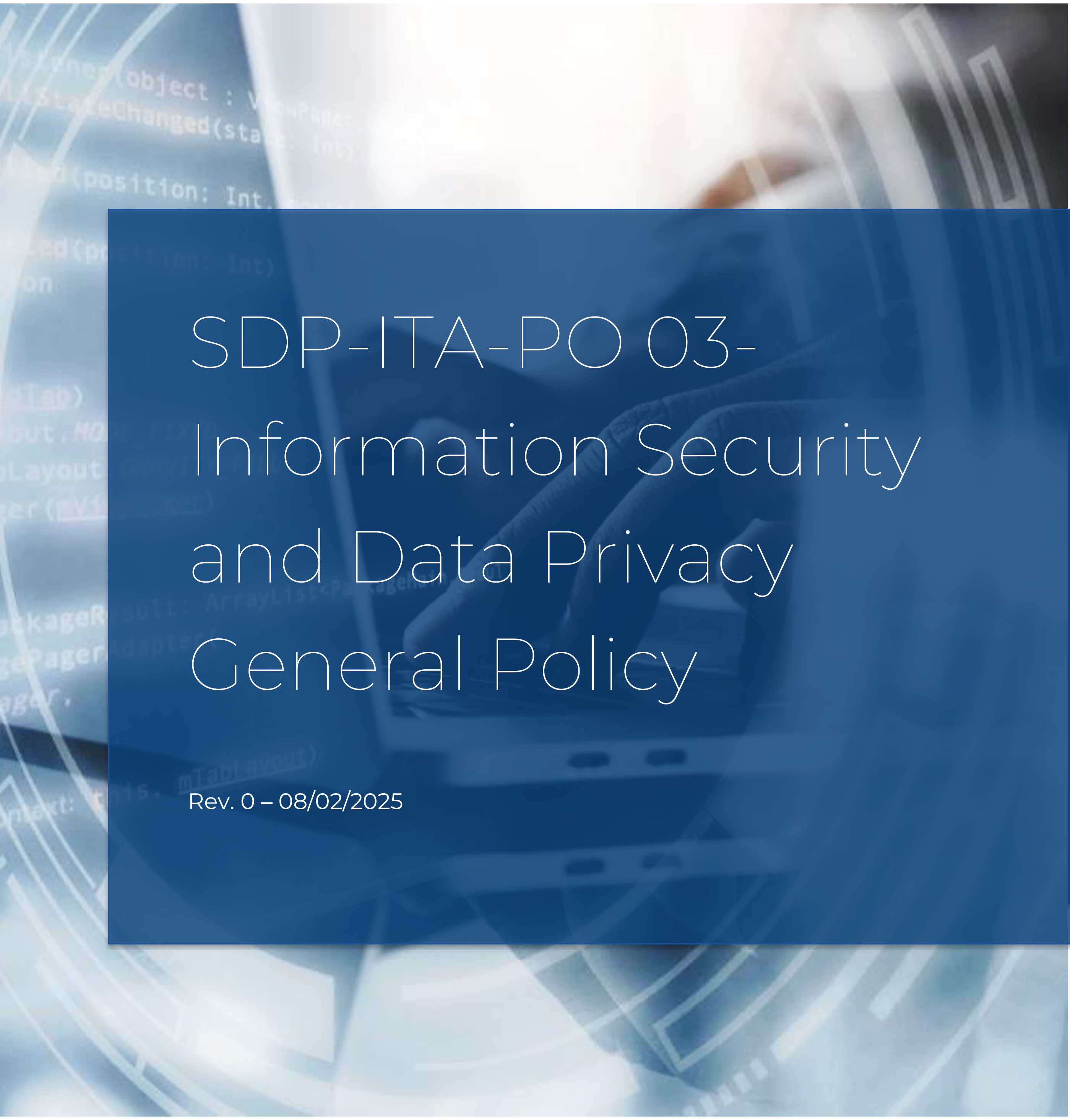
- **act with determination**, because quality and customer satisfaction are obtained only through concrete actions, with a constant commitment and a deep sense of responsibility of everyone of us;
- get it **right the first time**, with the aim of meeting product and service requirements, including applicable regulatori requirements;
- be **prompt in responding** to incidents and react with a **desire to remove** the real **cause** of it;
- act by implementing **careful and continuous prevention**, just as we do when our own interests are at stake;
- **be always aware of the repercussions** that **our actions** and decisions have on the other part of the organization;
- **consider as a "Customers" the colleague who receives the result of our work**: in fact customers are not only the end users, but also our colleagues, other departments in the organization and our external collaborators; we have to do our best to give them the best inputs, because if everyone of us do it this way, the overall result will be excellent and always the very maximum possible

- be aware that **poor adherence to** the product and service **specifications creates a high cost** for the organization, in terms of the need to fix products or **re-deliver services** and in terms of **loss of image in the** market.

We believe that **competitive advantage** in firmly linked to **intellectual capital** (to be achieved through continuous discussion and involvement of our employees in the internal processes and in the generation of solutions) **and** innovative business **organization**: we think that the most interesting minds are those that know how to unleash their imagination, ask new questions and find answers, face challenges and plot a new path for those who follow.

We believe that a successful business organization should be based on the **passion of** its people, on a continuous and effective internal communication, on the **tension to problem solving**, on the goal to produce **value and satisfaction** for its stakeholders and **the customer** in particular: in short, we want to be a strategic and irreplaceable partner and not just a simple supplier for our customers.

The TOP MANAGEMENT of DEDALUS ITALIA spa



SDP-ITA-PO 03- Information Security and Data Privacy General Policy

Rev. 0 – 08/02/2025

Changes from the previous published version are identified with a line in the margin as for these sample lines and documented in the revision history. Major versions do not show revisions tracked explicitly to ensure the readability of the document.

TABLE OF CONTENTS

1 SCOPE

This policy of is applicable to Dedalus Italia and to all the companies of the Dedalus group indicated in the governance record QARA-ITA-GR 01-Legal entities che hanno adottato l'IMS di Dedalus Italia (irrespective of sites, facilities and operations); in this document these companies are collectively referred to as "Dedalus".

This policy is also applicable to all staff, suppliers, contractors and consultants (irrespective of the nature or duration of their work or their geographic location), all solutions, products and services (irrespective of the form, the technology used, the physical location (on prem, private or public cloud) or the phase in the lifecycle of the solution, product or service in question).

The Information Security Management System (ISMS) is incorporated into the Integrated Management System (IMS) of Dedalus Italia.

2 PURPOSE

Dedalus is committed to support healthcare providers in protecting the personal data and especially the health data of their patients by delivering secure products and services.

This policy expresses the vision of Dedalus management on Information Security & Data Privacy (IS&DP). This would generally include protecting IT systems, user awareness on security and privacy, supplier management and other information security domains.

This document focuses on below information security domains corresponding to the ISO/IEC 27001:2022 clauses, and the related guidelines ISO/IEC 27017:2017 and ISO/IEC 27018:2019 for cloud:

- A.5 Organizational controls
- A.6 People controls
- A.7 Physical controls
- A.8 Technological controls

3 Policy

3.1 Policy Statements

Dedalus is a manufacturer of IT products. It is operating in a market with increasingly digitized and interconnected systems and more regulations and customer requirements.

3.1.1 Definition of the interested parties and their responsibilities

Dedalus ISMS is referred to all the interested parties, which are listed with their IS&DP requirements and expectations related to Dedalus ISMS:

Internal interested party	Requirements and Expectations of the Stakeholders to Dedalus ISMS
The Dedalus Italia Leadership Team (LT)	They define the objectives for the Dedalus ISMS and want to perform business with confidence and to be informed about the risks and impacts related to their decisions.
Dedalus IT Group	Need and ask for guidance on how: • to implement applications and infrastructure in a secure way • to ensure compliance with data privacy regulations for the storage of Personally Identifiable Information (PII), Protected Health Information (PHI) and other health data on Dedalus systems Provides cybersecurity services: • Handling of Dedalus internal security incidents • Supporting the management of security incidents in Dedalus cloud infrastructure as well as for customer on-prem installations

Internal interested party	Requirements and Expectations of the Stakeholders to Dedalus ISMS
	• Providing the tooling including the SIEM for security monitoring, detection, response and recover. • Providing the SOC service for Dedalus internal and cloud infrastructure
Sales	Need and ask for guidance on how: • to integrate IS&DP in their customer-facing sales and services activities in a resource-efficient manner (e.g. tender, contracts, customer requirements)
Order fulfilment / Program management	Need and ask for guidance on how: • to deploy, maintain and use products and tools in compliance with IS&DP regulations and best practices. • to ensure that security by design and privacy by design principles are followed when deploying software on-prem and in the cloud • to ensure the correct handling of PHI
Solution Development	Need and ask for guidance on: • how to build products that are in line with IS&DP regulations and best practices. • integrating IS&DP in their processes (e.g. data use, supplier management)
After Sales / Managed Services and delivery	Need and ask for guidance on how: • to support the customers on the use of products and tools in compliance with IS&DP regulations and best practices and • to manage complaints in compliance with IS&DP regulations and best practices. • to handle of customer related security incidents

Internal interested party	Requirements and Expectations of the Stakeholders to Dedalus ISMS
	• to ensure the correct handling of PHI
Global and local support function like HR, procurement	Need and ask for guidance on how to integrate transversal IS&DP requirements in their processes.
Data Protection Officer (DPO)	Need for defined controls and measures to ensure correct data privacy management of PII and PHI within Dedalus
Trade unions and workers' committees	Need for defined controls and measures to ensure correct privacy management of workers in the company of Dedalus
Workers (employees and collaborators in Dedalus)	Proper management of company tools and information Attention to the management of their data in compliance with applicable current privacy regulations Need and ask for guidance on confidentiality, availability, integrity of Dedalus' data.

External interested party	IS&DP requirements and expectations of the Stakeholders to Dedalus ISMS
Customers	Confidentiality, availability, integrity of information managed through software used by customers, independent if deployed on-prem or in the cloud, and through services, incl. cloud services, provided. Great attention to the management of sensitive health data of patients in compliance with all the applicable privacy regulations, GDPR and privacy regulations of non-European countries.
Users (people) of the services provided by Dedalus to the client (physicians, nurses, administrative staff, etc.)	Confidentiality, availability, integrity of the user data used or stored within Dedalus software, infrastructure and cloud services. Compliance with the applicable current data privacy regulations.
Patients	Confidentiality, availability, integrity of the patients PII and the health data used or stored within Dedalus software, infrastructure and cloud services.
Suppliers	Confidentiality, availability, integrity of suppliers' data used or stored within Dedalus software, infrastructure and cloud services. Compliance with Privacy regulations. Supporting of audits to ensure the required level for IS&DP is met within their perimeter and services.
The Data Protection Authorities of the countries in which Dedalus operates	Compliance of software and solutions with applicable international, national and local regulations and guidelines Increased security in the processing of data with the use of tools and services, incl. cloud service, developed/managed by Dedalus / the companies of the Dedalus

Certification bodies and regulatory authorities	They may audit or inspect Dedalus's IS&DP posture, periodically or unannounced and may depending on their mandate- impose enforcement actions, e.g. withdrawing a certificate, levying a fine, revoking the right to sell in a local market or banning a data processing activity
Investors in the Group and in the companies of the Group	Compatibility of Dedalus software and solutions with the privacy regulations and the provisions of the Privacy Guarantor, the GDPR and the regulations of the countries in which Dedalus operates. Increased security in data processing with the use of tools and services, incl. cloud services, developed/managed or used by Dedalus

3.1.2 ISMS Scope and Scope Exclusions

The scope of the ISMS is defined in IMS Handbook (paragraph 1) and in the governance record ISP-ITA-GR-01-Dedalus Italia Statement of Applicability (SoA), for an overview of controls in scope and controls excluded.

3.1.3 Information Security and Data Privacy Objectives

Dedalus is committed to support care providers in protecting the data privacy of their patients by delivering secure products and services; to do this the top management of Dedalus has defined the following objectives:

1. Ensuring regular reporting of information security KPIs to management and define the necessary follow-up actions
2. Establishing effective information security awareness, training, and education program, informing all employees and other relevant parties at all relevant levels of their information security obligations set forth in the information security policies, objectives etc., and motivating them to act accordingly
3. 90% completion of Dedalus Security Awareness Training for the employees of the companies in scope of the ISMS of Dedalus Italia defined in QARA-ITA-GR 01-Legal entities che hanno adottato l'IMS di Dedalus Italia

4. Minimizing the organization's exposure to information security risks
5. Implement the necessary technical protection and monitoring to avoid security incidents
6. Ensuring the best practices regarding secure coding, security by design and privacy by design are implemented within the development process
7. Actively ensuring the prevention and detection of information security incidents
8. Ensure compliance with data privacy and information security regulations which are applicable to our organization and customers.

3.2 Policy principles

In the ISO/IEC 27002:2022 standard (Information security, cybersecurity and privacy protection — Information security controls), there is a section mentioning five control attributes. Control attributes are used to categorize controls. Dedalus should use these attributes with values based on the organization's requirements to understand the current security posture. For detailed information on control attributes, please refer to the ISO/IEC 27002:2022 standard, and its guidelines for cloud and the guidelines ISO/IEC 27017:2017 and ISO/IEC 27018:2019 for cloud.

Below are the five control attributes along with their values:

1. **Control types**

Attribute values:

- Preventive (control to prevent the occurrence of information security incident),
- Detective (controls acts when an information security incident occurs)
- Corrective (controls acts after an information security incident occurs)

2. **Information security properties**

Attribute values:

- Confidentiality,
- Integrity and
- Availability

3. **Cybersecurity concepts**

Attribute values:

- Identify
- Protect
- Detect
- Respond
- Recover

4. Operational capabilities

Attribute values: Governance, Asset Management, Information protection, Human resource security, Physical security, System and network security, Application security, Secure configuration, Identity and access management, Threat and vulnerability management, Continuity, Supplier relationships security, Legal and compliance, Information security event management and Information security assurance.

5. Security domains

Attribute values:

- Governance and Ecosystem,
- Protection,
- Defence and Resilience

To fulfill information security objectives, Dedalus has adopted information security policy principles listed below that correspond to the ISO/IEC 27001:2022; this policy considers also the requirements of the guidelines ISO/IEC 27017:2017 and ISO/IEC 27018:2019 for cloud.

3.2.1 Organizational controls (A.5)

Organizational controls focus on the policies, processes, procedures, responsibilities and other organizational measures.

Total controls covered: 37

Policies for information security:

Dedalus must have in place IT security requirements and guidelines in order to secure IT systems in the organization. Detailed policies and procedures for information security must be defined, reviewed, approved by the information security process owner and communicated to employees and relevant external parties on a regular basis. Review of the Information Security and Data Privacy (IS&DP) Global policy and the procedures must be performed at least annually.

Information security roles and responsibilities:

Internal organization:

The Dedalus Italia Leadership Team (LT), led by the Dedalus Chairman, is accountable for corporate governance.

The management and control of IS and DP risks are an integral part of this corporate governance.

The LT gives overall strategic direction by approving and mandating through the CEO this SDP-ITA-PO 03-Information Security and Data Privacy General Policy, but delegates tactical responsibilities:

- to the CISO Office (ISO 270XX standard expert) in relation to the technical content of the Information security Management System and
- to the ISMS Manager in relation to the framework, which is part of Dedalus Italia’s overall Integrated Management System (IMS) managed by QARA.

To allow for an efficient and coordinated promotion, implementation and integration of this IS&DP policy, roles and responsibilities shall be defined and allocated in an organization. Segregation of duties shall be maintained to reduce risk of unauthorized modification or misuse of assets.

External organization:

Dedalus contractors and consultants shall adhere to and be informed about the IS&DP policy and process documents. Their employment terms and conditions shall include nondisclosure and confidentiality agreements and/or clauses.

- Asset management: This is to identify, protect, manage and secure all the assets in Dedalus. Assets associated with information and information system asset inventory shall be established and maintained. For each asset, or group of assets, a classification identification and ownership shall be identified and documented. Usage of corporate equipment by the employees should be handled in a secure manner. Ownership shall be assigned to an individual with adequate knowledge and its role in the business processes of Dedalus. Upon termination of employment, an employee shall return all organizational assets. To prevent unauthorized disclosure and modification, information shall be classified and labelled as per classification scheme adopted by Dedalus. Information stored on media should be managed as per Dedalus procedures and disposed securely when no longer required.

- Access control: To prevent unauthorized access to systems and services, access control should be documented and reviewed every year and would be outlined as part of the relevant Access Governance Procedures. Access to systems and network infrastructure services shall only be granted to authorized users. Assigning or revoking a user access right must be documented, managed, approved as per Access Governance Procedures document. User access recertification for both systems and network infrastructure services need to be performed on an annual basis. Unique individual usernames shall be allocated in order to allow for non-repudiation of information handling. Secure log in procedures, Segregation of duties and Password management system must be implemented for a secure access to systems. Use of privileged utility programs or program source code shall be restricted and closely controlled and monitored. Logging and tracking mechanisms shall be implemented. Access to both internal and external networked services shall be controlled, and strong authentication shall be implemented for secure access to applications and most importantly remote users. Connection to Dedalus's internal network via public network or dial-in shall be protected appropriately.

- Information security in supplier relationships: In order to ensure the supplier management process is performed in accordance to IS&DP requirements:
  - an IS&DP policy for the supplier shall be defined, to mitigate the risk of their access to Dedalus assets
  - contracts with third-party vendors shall include non-disclosure and confidentiality agreements and/or clauses
  - vendor contracts or agreements shall include clauses to manage risks of the supplier chain, whenever relevant and necessary.

- Information security incident management: IS&DP is established through the safeguarding of the confidentiality, integrity and availability of data and information systems. Any breach of one of these elements can be a threat to Dedalus, to the customer and data of Dedalus, and is considered as an IS&DP incident. An incident management system shall ensure the prompt, efficient and effective identification, assessment, communication, follow-up and timely resolving of incidents as well as the decrease or avoidance of similar incidents. Where possible, logging and tracking mechanisms shall be activated to help investigations on security incident. Security incidents should be managed, resolved and documented. Dedalus employees shall be informed about the nature of IS&DP incidents and the procedures to report them. They shall report any IS&DP incidents and any known or suspected vulnerabilities as soon as possible.

- Information security aspects of business continuity management: Disruption of the core activities, caused by major incidents or disasters, can have a significant economic and reputational impact on Dedalus. Special attention shall be given to:
  - business continuity threats during risk assessments for solutions
  - the continuity of aftersales processes where service level agreements with customers are present
  - the continuity of solution development processes
  - and in general, to the services under ISO 20000-1 certification and to the SaaS under ACN (Italian Agenzia per la cybersicurezza nazionale) qualification
  - Procedures on Business Continuity Management need to be documented and shall be planned, implemented, verified, reviewed and evaluated annually, also in accordance to the Business Continuity Management System of Dedalus developed for SaaS and in compliant to ACN qualification requirements.

- Compliance: Legal and contractual obligations as well as intellectual property rights and data privacy protection requirements shall be considered in all processes of the organization. In order to ensure this, requirements and obligations shall be clearly identified and considered during the development of the IS&DP policies and process documents. To ensure compliance with Dedalus's IS&DP policy, regular verifications and audits are required. Systems and processes shall be analyzed to ensure they meet the expected IS&DP levels.

- Documented operating procedures: To ensure the correct and secure operation of information systems, process documents shall be established. No evidence is required for aspects which are reasonably expected to be known by employees through their logical or repeated use or deduction.

  Special attention shall be given to document processes and/or procedures in the area of:

  – day-to-day operational service

  – processing, accessing, exchanging and removing sensitive information

  – management of logs and audit trails

  Where possible, segregation of duties shall be established and documented.

- Information transfer: To ensure that the information is protected in the network and secured during information transfer within or outside the organization.

  Special attention shall be given to document processes and/or procedures in the area of:

  – information transfer policy and procedure

  – confidentiality and non-disclosure agreement for protecting confidential information and information transfer within and outside the organization.

- Threat intelligence: To provide awareness of the organization's threat environment so that appropriate mitigation actions can be taken. Information relating to information security threats should be collected, analyzed and contextualized data about current and future cyber-attacks to produce threat intelligence.

- Information security for use of cloud services: To specify and manage information security for the use of cloud services. Cloud service agreements should be defined and reviewed with the cloud service provider.

Special attention shall be given to document processes and/or procedures in the area of:

- Information security requirement for cloud services
- Define and document the scope, roles and responsibilities and management of cloud services
- information security controls managed by cloud service provider and/or cloud service customer
- perform risk assessments to identify information security risks and residual risks associated with cloud service
- handle information security incidents that occur with the use of cloud services
- review and monitor the ongoing use of cloud services to manage information security risks
- process to change or stop cloud service usage.

To implement the management of SaaS provided to its customer Dedalus ISMS is designed and implemented in compliance with ISO 27017 and ISO 27018 guidelines, as well to meet the requirements of ACN qualification.

- ICT readiness for business continuity: Dedalus shall define recovery time objective (RTO) and business impact analysis (BIA) to ensure the availability of the organization's information and other associated assets during disruption. The business continuity management system for SaaS service provided to Dedalus customer, shall be compliant with ISO/IEC 27017:2017 and ISO/IEC 27018:2019 and also to the standards define in the Business Continuity Management System part of the IMS of Dedalus.

3.2.2 People controls (A.6)

People control focuses on human resource management, personnel security and security awareness training.

Total controls covered: 8

Human resource security: This security is to ensure that the employees understand their roles and fulfill their information security responsibilities. Specific guidelines shall be implemented to ensure IS&DP during the following phases of employment:

- Prior to employment
- During employment
- Termination and change of employment

3.2.2.1 Prior to employment

After hiring, employees shall be informed about IS&DP responsibilities of their role in their function and in the organization. Possible disciplinary action in case of non-compliance with the IS&DP policy of Dedalus shall be communicated. Their employment terms and conditions shall include non-disclosure and confidentiality agreements and/or clauses.

3.2.2.2 During employment

Employees of Dedalus shall be made aware of their IS&DP roles and responsibilities Adequate security awareness training and instructions shall be provided. Especially those employees with access to Dedalus data such as sensitive information, i.e. PHI, security information, PII, Intellectual property and other company-related information shall be informed about the private and confidential nature of this data and the impact if the information is not handled appropriately. Initiatives shall be taken to ensure the establishment and maintenance of IS&DP awareness throughout Dedalus. There should be a formal disciplinary process in place to take action against employees who have committed information security breaches. There are information security implications for remote working that should be considered and documented. The remote working policy should outline where and when remote working is permitted, device provision, authorized access and what information may be accessed remotely.

3.2.2.3 Termination and change of employment

When an employee takes up another position within Dedalus or leaves Dedalus, necessary actions shall be taken to ensure the continued protection of data. When leaving Dedalus or when changing positions, assets owned and provisioned by Dedalus shall be returned. Access to both physical and software infrastructure of Dedalus needs to be revoked immediately after the last working day of an employee to ensure data protection and integrity.

3.2.3 Physical controls (A.7)

Physical control focuses on protecting tangible assets from physical threats.

Total controls covered: 14

Physical security:

- Physical entry controls should be in place to allow only authorized users to access sites and offices of Dedalus. Logs shall be maintained and monitored for all unauthorized persons entering the premises for traceability purposes in the event of a physical security breach. User access recertification for physical infrastructure needs to be performed on an annual basis.
- Physical premises should be monitored by:
    - surveillance systems (e.g., security guards, intruder alarms, video monitoring systems and CCTV)
    - continuous monitoring systems (e.g., CCTV, contact detectors, motion detectors and sensors sensitive to the sound)
    - anti-intrusion system to notify of any unauthorized intrusion outside business hours.

Environmental security: Information and information systems shall be protected against theft, loss, damage of assets through prevention, detection or protection mechanism in case of fire, theft or loss, water damage and an adequate alternative power supply or other measures to prevent disruption of committed (e.g. through Service Agreements) services. There must be plans implemented during power failure and other disruptions to ensure equipment availability to Dedalus users. Wherever cabling is located, the rooms or cable cabinets shall be locked and assigned security access areas. A clean desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted. A clean desk and clear screen work instruction shall be adopted to safeguard storage media and information processing facilities.

3.2.4 Technological controls (A.8)

Technological controls focus on controls required to set up and maintain secure technological systems, development and code management.

Total controls covered: 34

- Cryptography: There shall be a policy defined on cryptographic controls to protect the information within Dedalus. These controls help to achieve information security objectives such as confidentiality, integrity and authentication. All cryptographic keys shall be managed and protected against unauthorized use and disclosure.

- Operations security: To ensure the correct and secure operation of information systems, process documents shall be established.

  Special attention shall be given to document processes and/or procedures in the area of:

  – change management activities on processes

  – staging and configuring systems

  – protection against viruses and malicious code

  – security attacks like phishing, vishing and smishing

  – managing technical vulnerabilities of information systems

  – roll-out of new software or updates on customer's infrastructure

  – backup

  – SaaS services

  Where possible, segregation of duties shall be established and documented.

- System acquisition, development and maintenance: Software Development Life Cycle (SDLC) controls, Test and Deployment controls and Emergency change management should be defined, reviewed, approved and documented annually. Where possible, segregation of duties shall be established and documented.

  Within Dedalus two kinds of information systems can be distinguished:

- internal applications (both on premise and on cloud): those used to ensure smooth operations of the different business and supporting processes within Dedalus
- customer products and services: those information systems which are designed and built for the support of the businesses within the Group domain.

Both shall adhere to sound IS&DP principles, in particular:

- a strong secure development procedure shall be active
- secure system engineering principles shall be defined and applied
- outsourced system development activities shall be strictly monitored and controlled

Internal applications:

Information security requirements shall be documented in the specifications of new, or to be modified, information systems and applications. These requirements shall be in line with the private and confidential nature of the processed or stored information and in line with the principles dictated by this document and by regulatory requirements. Special attention shall be given to e.g.

- means to protect the confidentiality, integrity and availability of data in transit
- strong access control (authentication and authorization) to data based on the least-privilege principle
- availability of the application and the information
- protected audit and logging for the creation, consultation, modification and deletion of data
- applications managed within a cloud environment

Similar considerations shall be made when evaluating a third party's information system and/or application.

Uncontrolled usage of data is not allowed in the development or test environment. Test data shall be made anonymous wherever possible or must be pseudonymised if anonymization is not possible. This operation shall be done in a secured area in the original environment where data are stored, always before importing data in the system.

The principles of access control shall be applied both in the development and test environment.

Customer products and services:

In order to deliver secure products and services to our customers, IS&DP measurements or controls shall be included in these products and services as of requirements and design phase. Following IS&DP controls shall be considered:

- means to protect the confidentiality, integrity and availability of data in transit
- availability measurements to ensure that the data is available when needed
- strong access control (authentication and authorization) to data based on the least-privilege principle
- protected audit and logging for the creation, consultation, modification and deletion of data

- Network security: To ensure that the information is protected in network and secured during information transfer within or outside the organization.

  Special attention shall be given to document processes and/or procedures in the area of:

  - network controls to manage and protect information
  - security of all network services
  - segregation in networks (information systems, users and information services)
  - information transfer policy and procedure
  - confidentiality and non-disclosure agreement for protecting confidential information and information transfer within and outside organization.

- Configuration management: Configurations including security configurations of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed. The organization should define and implement processes and tools to enforce the defined configurations (including security configurations) for hardware, software, services (e.g. cloud services) and networks for newly installed systems and operational systems. Roles, responsibilities and procedures should be in place to ensure adequate control of all configuration changes. Changes to configurations should follow the change management process.

- Information deletion: Information stored in information systems, devices or in any other storage media should be deleted when no longer required taking into consideration relevant legislation and regulations. When deleting information on systems, applications and services, the following measures should be considered:
  - selecting a deletion method (e.g. electronic overwriting or cryptographic erasure) following the business requirements and relevant laws and regulations
  - recording the results of deletion as evidence
  - obtaining evidence of information deletion from the supplier when using service suppliers of information deletion

- Data masking: To limit the exposure of sensitive data including PII and to comply with legal, statutory, regulatory and contractual requirements, data masking techniques like pseudonymization or anonymization, encryption, etc. should be implemented.

- Data leakage prevention: To reduce the risk of unauthorized disclosure and extraction of information by individuals or systems, Dedalus should consider the following measures:
  - identifying and classifying information to protect against leakage (e.g. personal information, test designs, health information, etc.)
  - monitoring channels of data leakage (e.g. email, file transfers, mobile devices and storage devices)
  - act to prevent information from leaking (e.g. quarantine emails containing sensitive information, classify files and emails based on the data content).

- Monitoring activities: Dedalus must promote a proactive approach to monitoring that aims to prevent and take actions to evaluate potential security incidents before they occur.

- Web filtering: Dedalus must implement appropriate web filtering controls to restrict and control access to external websites and prevent security threats and risks like malware infection from accessing external websites with malicious content. The organization needs to identify high-risk external websites and implement appropriate access and web filtering controls.

- Secure coding: Dedalus needs to follow secure coding principles to prevent security risks and vulnerabilities that may arise due to poor software coding practices.

3.3 Obligations

This policy imposes the following obligations:

- securing the Dedalus data such as security information, Personally Identifiable Information (PII), Protected Health Information (PHI), Intellectual property and other company related information
- securing the Products for our customers
- securing the Software as a Service services provided to our customers
- securing the Technical and Professional Services for our customers
- securing the Dedalus IT Group Services
- securing the Dedalus core Processes

4 Applicable Standards & Regulations

This policy is compliant with the following standards:

Standard/Regulation/Guidance/Requirement	Title
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements
ISO/IEC 27017:2015	Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018:2019	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27001:2022 is an international standard to provide requirements for establishing, implementing, maintaining and continually improving an information security management system, preserving the confidentiality, integrity and availability of information by applying a risk management process and giving confidence to interested parties that risks are adequately managed. The application of this standard helps to ensure implementation of end-to-end information security policies within an organization; this policy are strategic for any IT organization.

ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002;
- additional controls with implementation guidance that specifically relate to cloud services.

It provides controls and implementation guidance for both cloud service providers and cloud service customers.

ISO/IEC 27018:2019 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

In particular, this document specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

It is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations; the guidelines in this document can also be relevant to organizations acting as PII controllers. PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors.

4.1 Applicable Processes and/or Methodologies

4.1.1 Deming cycle

To implement this policy and the whole ISMS, Dedalus has adopted a global risk-based approach to information security in line with the Plan-Do-Check-Act (PDCA) process as part of the Integrated Management System of Dedalus Italia.

4.1.2 Best practices

In addition to the standard above listed, Dedalus shall consider the following security & privacy best practices:

- ISO/IEC 27002:2022 Information technology – Security techniques – Code of practice for information security management
- ISO/IEC 27799:2016 Health Informatics – Information Security Management in Health using ISO/IEC 27002
- ISO/IEC 27005:2019 Information technology – Security techniques – Information security risk management
- Health Insurance Portability and Accountability Act (HIPAA)

4.2 Accountability

Type of accountability	ACCOUNTABLE FUNCTION
STRATEGIC	Dedalus Italia Chairman Leadership Team Members
TACTICAL	Policy, technical guide & baselines: • BPO • CISO Office • Product Security Office (PSO) • Technology and Architecture Office (also called CTO)
	System framework: • ISMS Manager
OPERATIONAL (organization, process, procedures, work instructions)	Regional GM and Management Team (Region) Business Unit Management (Global and local) Sales & services Organization Manager (Regions) Support Function Manager (MarCom, QARA, Legal, HR, Procurement, DITG, CISO Office, PSO Office, CTO Office, Enterprise Risk and Compliance, DPO and DPM)

Accountable Management may delegate responsibilities but cannot transfer their ultimate accountability.

5 Definitions & References

Acronyms

Terminology	Explanation
BPM	Business Process Manager
BPO	Business Process Owner
GSS	Global Support Service
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resource
IMS	Integrated Management System
IS&DP	Information Security and Data Privacy
ISMS	Information Security Management System
IT	Information Technology
LT	Leadership Team
PHI	Protected Health Information
PII	Personally Identifiable Information
QARA	Quality Assurance, Regulatory Affairs
SA	Service Agreement
SDLC	Software Development Life Cycle

Definitions

Terminology	Explanation
Business Continuity management (BCM)	BCM provides the organization with the ability to effectively respond to threats such as natural disasters or data breaches and protect the business interests of the organization without going out of business
Contractual obligation	It refers to rights and duties that both parties are legally responsible for in a contractual agreement
Cryptography	cryptos + graphy means hidden writing. It is a practice to protect information and communication using algorithm so that only those for whom the information is intended can read and process it.
Digital certificates	It is an electronic file that is used to verify the identity of a party on the Internet and enables encrypted connections. In simple terms, digital certificates are like electronic passport.
Health Insurance Portability and Accountability Act (HIPAA)	USA Federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge
Other company data	Company data contains information which are confidential and critical to normal functioning of Dedalus. This information includes all company related data e.g. internal documents, communication, etc.
Personally Identifiable Information (PII)	Personally Identifiable Information (PII) is any information relating to an identified or identifiable natural person. This information includes social security number, phone number, email address, online identifiers etc.
Phishing	Phishing is a type of social engineering attack where an attacker calls or sends a fraudulent email or message

Terminology	Explanation
	designed to lure individuals into revealing sensitive information.
Products	Dedalus products, internal tools, internal IT infrastructure components, customer systems (comprising of Dedalus products and Third-party products)
Protected Health Information (PHI)	Protected Health Information (PHI) is any individually identifiable information related to physical or mental health status of an individual or provision of health care or payment for healthcare. In this document and all the IS&DP documents this term is used and includes: - Health Data - PID (Patient Identifiable Data) (https://en.wikipedia.org/wiki/Protected_health_information)
Security information (SI)	Security Information is the whole of sensitive security and network settings and of communication, software or hardware tools which control access to a system containing PHI or provide means to alter the system's integrity or behavior, e.g.: passwords, configuration data, communication parameters, security software
Segregation of duties	This concept ensures that no one person should be assigned responsibility for multiple tasks linked to each other.
Smishing	SMS + Phishing = Smishing. An attacker sends a text message to provoke recipients into clicking a link or downloading an application and thereby sending the attacker private information or downloading malicious programs to a smartphone.
Software Development Life Cycle (SDLC)	A methodology describing the software application lifecycle. Planning -> Analysis -> Design -> Implementation -> Testing -> Maintenance

Terminology	Explanation
Vishing	Voice + Phishing = Vishing. An attacker convinces an individual to provide sensitive information over the telephone.

5.1 References

Reference name	Reference ID / Location
ISP-ITA-GR-01-Dedalus Italia Statement of Applicability (SoA)	SharePoint of the IMS of Dedalus Italia

6 ANNEX

6.1 Detailed IS&DP Roles and Responsibilities

6.1.1 Dedalus Leadership Team (LT)

The Dedalus Leadership team (LT), led by the Dedalus Italia CEO, is **ultimately accountable for Dedalus Information Security corporate governance**.

The management and control of IS&DP risks is an integral part of this corporate governance.

The Leadership Team gives overall strategic direction by approving and mandating this SDP-ITA-PO 03-Information Security and Data Privacy General Policy (IS&DP policy), but delegates tactical responsibilities to CISO office, which is guided by the BPO Information Security and Data Privacy, the CEO of Dedalus Italia (LT delegate for Information Security and Data Privacy).

The Leadership team IS&DP responsibilities shall be at least:

- outline the IS&DP policy of Dedalus;
- approve, support and commit to the IS&DP policy of Dedalus;
- provide adequate expertise to implement and maintain an efficient and effective IS&DP policy;
- conduct regular IS&DP reviews;
- review and discuss critical or non-acceptable IS&DP incidents, problems or risks.

6.1.2 CISO Office

The CISO Office is responsible for the tactical IS&DP responsibilities in relation to policies, technical guide & baselines.

These shall be at least:

- develop strategic IS&DP policy, global guide- & baselines and work instructions;
- ensure IS&DP training is developed and maintained;
- monitor and assess the status of the IS&DP policy and IS&DP incidents within Dedalus;
- manage – in close cooperation with QARA and the – the IS&DP Risk Management process;

- where needed escalate critical risks into the Corrective And Preventive Action (CAPA) process;
- report the status of the IS&DP policy and IS&DP incidents to the security committee and to the LT.

6.1.3 Technology and Architecture Office (CTO)

The Technology and Architecture Office (CTO) is responsible for some tactical IS&DP responsibilities:

- develop and constantly evolve the Dedalus Reference Architecture (DRA) for the software applications
- develop and constantly evolve the Dedalus Security Framework (DSF) for the software applications
- identify and provide the tools to support the above activities
- formalise and document the DRA and the DSF
- ensure training of development teams is relation to the architectures and frameworks identified
- assess the existing products in relation to their adherence to the architecture and framework defined
- early identify the new regulations (in particular National and European ones) to ensues continuous compliance of Dedalus products architecture and security framework.

6.1.4 Business Units, Sales, Order Fulfilment, After Sales and other business processes of Dedalus Operating Model

The Director / Business Owners identified as the first report line of the CEO in the current Organisational Chart are responsible for implementing IS&DP controls.

They shall have at least the following responsibilities:

- design, review and adjust the IS&DP policy and process documents of Dedalus Italia and their implementation;
- review and discuss IS&DP incidents and problems and propose solutions to the LT when critical IS&DP incidents, problems or risks occur;

- review and adopt in the IS&DP policy any relevant changes in healthcare laws and regulations;
- formalize the ownership of global information and information systems.

They are IS&DP Risk Owner for their process and shall be at least:

- participate in the risk assessment coordinated by QARA;
- evaluate the risks related to their process / area;
- actively contribute to manage IS&DP risks in accordance to the current IS&DP risk methodology.

6.1.5 Management of Business Units, Sales, Order Fulfilment, After Sales and other business processes of Dedalus Operating Model

Management is accountable for day-to-day IS&DP activities and for compliance within his/her area of authority.

Business Units, Sales, Order Fulfilment, After Sales and other business processes Management shall have at least the following responsibilities:

- address/communicate the IS&DP policy and process documents of Dedalus Italia prior to and during employment, to subordinates;
- coordinate and monitor IS&DP training for his/her employees;
- ensure implementation of and compliance with the IS&DP policy, its global minimum baseline requirements and process documents;
- implement the IS&DP process documents in the organisation they lead;
- communicate the creation, modification or removal of access rights of an employee via the proper channel.
- contribute to the evaluation of the IS&DP risks in accordance to the current IS&DP risk methodology.

6.1.6 Owners of information and information systems

Owners are accountable for the IS&DP of the information and/or information systems they manage.

Their responsibilities shall be at least:

- classify the information and information systems;
- apply the IS&DP policy and process documents of Dedalus Italia to their day-to-day activities;
- cooperate with the planning, development and execution of the business continuity planning;
- plan and develop acceptance tests for applications;
- approve or deny access to confidential information;

6.1.7 Employees and Contractors

Employees shall make IS&DP an integral part of the quality of Dedalus’s products and services and of the organization and operations. They shall learn and adopt IS&DP in their professional activities.

Dedalus employees shall have at least the following responsibilities:

- become familiar with IS&DP policies and process documents of Dedalus Italia that are relevant for their role;
- comply and commit to the IS&DP policy and process documents of Dedalus Italia when performing day-to-day activities;
- safeguard IS&DP in day-to-day activities;
- abide by the code of conduct;
- report IS&DP incidents or weaknesses to the Service Desk;
- attend IS&DP awareness initiatives;
- cooperate with (internal or external) IS&DP audits.

6.1.8 Quality Assurance Regulatory Affairs (QARA)

The ISMS is incorporated in the Integrated Management System (IMS) of Dedalus.

The ISMS needs shall be addressed in the IMS and its processes.

QARA is responsible through the ISMS Manager to ensure the framework of the ISMS is fully integrated in the IMS framework.

QARA shall also work with the process owners and manager to ensure that they have implemented and maintained the selected IS&DP controls in Dedalus's processes, applications and information systems.

QARA is responsible to maintain the ISO 27001 certification with all the relevant extensions ISO/IEC 27017 and ISO/IEC 27018, recurrent audits are planned and executed by QARA.

The responsibilities of QARA include:

- gain knowledge of the IS&DP policy and process documents of Dedalus Italia and about the selected ISO 27001 controls with all the relevant extensions ISO/IEC 27017 and ISO/IEC 27018;
- develop and follow-up the audit plan;
- report any non-conformities, observations and/or recommendations to the LT;
- inform any non-conformities, observations and/or recommendations to process owners and stakeholders that should follow up or that are impacted.

As business and regulatory requirements continuously evolve, Dedalus shall ensure that the information security risks its business is facing are appropriately identified by Risk owners.

Therefore, QARA shall coordinate the execution of recurrent IS&DP risk assessments by the appropriate risk owners, in strict cooperation with and involvement of CISO Office.

The responsibilities of the IS&DP Risk Process manager shall be at least:

- coordinate IS&DP risk assessments;
- participate in the risk assessment;
- report on the status and the IS&DP level to stakeholders that should follow up or that are impacted;
- recommend possible risk treatment improvements.

6.1.9 Legal

To comply with privacy and security legislations that are applicable to Dedalus, its customers or its suppliers, local legislative requirements shall be monitored and where needed incorporated in Dedalus's processes.

The Legal Team's responsibilities shall be at least:

- identify, maintain and communicate IS&DP legislations;
- provide feedback to questions with respect to:

  - IS&DP questions in third-party agreements;
  - local healthcare and cryptography legislations.

6.1.10 Human Resources

To ensure that all employees are informed about and understand IS&DP, Human Resources (HR) shall assist line manager with the implementation of specific IS&DP measurements and guidelines.

HR shall be responsible at least for:

- addressing IS&DP prior, during and after employment;
- addressing IS&DP in the terms and conditions of employment;
- organizing IS&DP awareness and training for all employees;

6.1.11 Dedalus GSS

Dedalus Global Shared Services (GSS) are responsible for providing services to Dedalus satisfying Dedalus's IS&DP requirements.

6.1.12 Third Parties

Some third parties (i.e., suppliers) play a vital role in the support and maintenance of Dedalus's commercial products. Therefore, they shall adhere to the IS&DP policy as set forth by Dedalus.

Third parties shall be responsible at least for:

- adhere to the IS&DP requirements as per third party agreements.