

	Information Security Policy	09-09-2026 Page 1 of 22
Classification: Public	SGSI 01	Version 1.2

Version control

Version	Reason	Prepared by	Date
0.9	Preliminary version.	External consultant	29-10-2025
1.0	Initial Version	Security Officer	13-11-2025
1.1	Adjustments and corrections	Security Officer	04-05-2026
1.2	Re-indexing of table of contents	Security Officer	09-09-2026

Approved by: Management on 17-07-2026

	Information Security Policy	09-09-2026 Page 2 of 22
Classification: Public	SGSI 01	Version 1.2

Contents

Introduction	3
Definitions.....	3
Purpose	4
Scope	4
Objectives or Mission of the Organisation	5
Foundations of this Policy	5
Security Requirements	7
Organisation and implementation of the security process	7
Risk analysis and management. Inclusion of risks involving Personal Data	7
Legal Requirements and regulatory framework	12
Roles, Responsibilities and Duties	13
Users	13
Information Officer (National Security Scheme)	14
Service Officer (National Security Scheme)	14
Management.....	14
Security Officer	15
Data Protection Officer	17
System Officer	17
System Security Administrator	18
Information Security Committee	19
Appointment and conflict resolution procedure	20
Personal Data	20
Third parties	21
Third parties as outsourced Security services	21
ISMS Development, Review and Audits	22

	Information Security Policy	09-09-2026 Page 3 of 22
Classification: Public	SGSI 01	Version 1.2

Introduction

This document sets out the Information Security Policy of Layers of Reality as the set of basic principles and lines of action to which the organisation commits, within the framework of the National Security Scheme (Esquema Nacional de Seguridad, ENS).

Information is a critical, essential and highly valuable asset for the activity of Layers Of Reality. This asset must be adequately protected, through the necessary security measures, against any threats that may affect it, regardless of the formats, media, means of transmission, systems or persons involved in its knowledge, processing or handling.

Information Security is the protection of this asset, with the aim of ensuring the quality of the information and business continuity, minimising risk and maximising the return on investments and business opportunities.

Information security is a process that requires technical and human resources and proper management and definition of procedures, in which the fullest collaboration and involvement of all Layers Of Reality personnel is essential.

The management of Layers Of Reality, aware of the value of information, is deeply committed to the policy described in this document.

Definitions

- **Information System:** an organised set of resources enabling information to be collected, stored, processed or handled, maintained, used, shared, distributed, made available, presented or transmitted.
- **Risk:** an estimate of the degree of exposure to a threat materialising on one or more assets and causing damage or harm to the organisation.
- **Risk management:** coordinated activities to direct and control an organisation with regard to risks.
- **Information Security Management System (ISMS):** a management system, based on the study of risks, established to create, implement, operate, monitor, review, maintain and improve information security. The management system includes the organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.
- **Availability:** the property or characteristic of assets whereby authorised entities or processes have access to them when required. It must be ensured that system resources will be available when needed, especially critical information.

	Information Security Policy	09-09-2026 Page 4 of 22
Classification: Public	SGSI 01	Version 1.2

- **Integrity:** the property or characteristic whereby the information asset has not been altered in an unauthorised manner. System information must be available exactly as it was stored by an authorised agent.
- **Confidentiality:** the property or characteristic whereby information is neither made available nor disclosed to unauthorised individuals, entities or processes. Information must only be available to authorised agents, especially its owner.
- **Authenticity:** the property or characteristic whereby an entity is who it claims to be, or which guarantees the source from which data originate. The identity or origin of the information must be ensured.
- **Traceability:** the property or characteristic whereby the actions of an entity (person or process) can be traced indisputably back to that entity. For certain data, it must be possible to establish who did what and when.

Purpose

The purpose of this Information Security Policy is to protect the information assets of Layers Of Reality by ensuring the availability, integrity, confidentiality, authenticity and traceability of the information and of the facilities, systems and resources that process, manage, transmit and store it, always in accordance with business requirements and current legislation.

Scope

This Information Security Policy applies to all persons, systems and media that access, process, store, transmit or use information known to, managed by or owned by Layers Of Reality for the services of: a) conceptualisation and design of immersive experiences; b) installation of audiovisual, interactive and immersive systems and software integration; and c) comprehensive control of the experience, commissioning and monitoring of production and operation.

The personnel subject to this policy include all persons with access to the information described, regardless of the automated or non-automated medium on which it is held and of whether or not the user is an employee of Layers Of Reality. It therefore also applies to any other third party with access to the information or systems of Layers Of Reality.

To ensure that the security process in place is continuously updated and improved, an Information Security Management System is implemented and documented. In this way, the content of this Information Security Policy is developed through complementary security standards and procedures.

	Information Security Policy	09-09-2026 Page 5 of 22
Classification: Public	SGSI 01	Version 1.2

Objectives or Mission of the Organisation

Layers of Reality is an augmented reality content creation studio that produces memorable, meaningful and transformative experiences for as many people as possible, regardless of their technological knowledge, age or social background. Our mission is to create immersive, memorable and transformative experiences through augmented reality and cutting-edge interactive technologies. We believe in breaking down barriers and making the digital world accessible to everyone, regardless of age, background or level of technological knowledge. Our goal is to develop engaging and meaningful content that connects people with unique, multisensory experiences that enrich their understanding and appreciation of the world around them.

Whether through art, culture or innovation, we are committed to exploring new dimensions of storytelling, pushing the boundaries of reality and offering every individual the opportunity to connect with the future in an inclusive and impactful way.

Foundations of this Policy

The ultimate objective of information security is to ensure that an organisation can meet its objectives, perform its functions and exercise its competences using information systems. Accordingly, the following basic principles shall be taken into account in matters of information security:

Security as a comprehensive process.

Security must be understood as a process made up of all the technical, human, material and organisational elements related to the system.

Awareness shall be promoted among the people involved in the process and their line managers, so that neither ignorance, nor lack of organisation and coordination, nor inadequate instructions become a source of security risk.

Risk-based security management.

Risk analysis is an essential and continuous part of the security process. Managing these risks will make it possible to maintain a controlled environment, with risks kept at acceptable levels, and will be carried out by applying security measures proportionate to the nature of the information processed and the services to be provided.

Prevention, detection, response and preservation.

System security includes measures that implement prevention, detection and response to security incidents, as well as the preservation of information and services should an incident occur.

Existence of lines of defence.

	Information Security Policy	09-09-2026 Page 6 of 22
Classification: Public	SGSI 01	Version 1.2

Layers Of Reality implements a protection strategy based on multiple layers, made up of organisational, physical and logical measures, so that when one of the layers fails, the system in place makes it possible to:

- Gain time for an adequate reaction to incidents that could not be prevented.
- Reduce the likelihood of the system being compromised as a whole.
- Minimise the final impact on it.

Lines of defence must consist of organisational, physical and logical measures.

Continuous monitoring and periodic reassessment.

Continuous monitoring will enable anomalous activities or behaviour to be detected and responded to in a timely manner.

Layers Of Reality implements regular security checks and assessments (including routine assessments of configuration changes) in order to know the security status of the systems at all times in relation to manufacturers' specifications and to the vulnerabilities and updates affecting them, reacting diligently to manage risk in light of their security status. Before any new elements, whether physical or logical, are introduced, formal authorisation will be required.

Likewise, it will request periodic reviews by third parties in order to obtain an independent assessment.

Security measures will be assessed and updated periodically, adapting their effectiveness to the evolution of risks and protection systems, and may lead to a rethink of security if necessary.

Segregation of responsibilities.

Layers Of Reality has organised its security by engaging all members of the company through the appointment of different security roles with clearly differentiated responsibilities, as set out later in this document.

Information systems shall distinguish between:

- The person or persons responsible for the information, who determine the security requirements of the information processed;
- The person or persons responsible for the service, who determine the security requirements of the services provided;
- The person responsible for the system, who is responsible for the provision of the services; and

	Information Security Policy	09-09-2026 Page 7 of 22
Classification: Public	SGSI 01	Version 1.2

- The person responsible for security, who takes the decisions needed to meet the security requirements.

Where personal data are processed, the DPO(s) (data protection officer), the data controller(s) and the data processor(s) shall also be identified, as appropriate.

Security Requirements

This security policy will be developed by applying the following requirements:

Organisation and implementation of the security process

Information security involves all members of the organisation. Layers Of Reality identifies those responsible and sets out their responsibilities for this purpose in the sections "Roles, responsibilities and duties" and "Third parties" of this document. This Security Policy and the related regulations shall be made known to all persons within the scope of this document.

Risk analysis and management. Inclusion of risks involving Personal Data

Knowing the risks and drawing up a strategy to manage them properly is paramount for Layers Of Reality, since only by knowing the security status can the appropriate decisions be taken to mitigate the risks it faces.

Where an information system processes personal data, the provisions of the GDPR and the LOPDGDD shall apply or, where applicable, Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties. The controller or processor, advised by the data protection officer, shall carry out a risk analysis in accordance with Article 24 of the General Data Protection Regulation and, in the cases set out in Article 35 thereof, a data protection impact assessment. Additional measures to be implemented may result from that analysis.

Layers Of Reality uses the **Magerit** methodology to analyse risks, carrying out a detailed analysis of the risks affecting the assets listed in an asset inventory, which is documented in a Risk Analysis document.

The entity determines the risk levels above which it takes treatment actions. A Risk is considered acceptable when implementing further security controls is estimated to consume more resources than the potential associated impact.

	Information Security Policy	09-09-2026 Page 8 of 22
Classification: Public	SGSI 01	Version 1.2

The Security Officer shall be responsible for ensuring that the risk analysis is carried out, and for identifying gaps and weaknesses and reporting them to the Information Security Committee.

This analysis shall be repeated:

- Regularly, at least once a year.
- When the information handled and/or the services provided change significantly.
- When a serious security incident occurs or serious vulnerabilities are detected.

Once the risk assessment process has been carried out, the management of Layers Of Reality is responsible for approving the residual risks and the risk treatment plans.

As regards the measures implemented under the ENS, if the risk analysis establishes more stringent measures, these shall be added to those described in the ENS.

Personnel Management.

All Layers Of Reality personnel involved with information and systems are trained and informed of their duties and obligations regarding security, essentially through the rules on the use of assets. Their actions are supervised according to the established roles to verify that the defined procedures are followed.

User access is unique, and users' rights and their activities relating to Information Security are periodically verified in order to correct or, where appropriate, demand accountability.

Professionalism, Awareness and Training.

Systems security is managed and reviewed by qualified Layers Of Reality personnel and specialised external personnel, who receive and update the training needed to ensure information security throughout the life cycle of the information systems: planning, design, acquisition, construction, deployment, operation, maintenance, incident management and decommissioning. Qualification requirements (training and experience) shall always be set by Layers Of Reality.

This Information Security Policy must be known to all internal and external users and to any companies that access, manage or process data of Layers Of Reality.

The set of Policies, standards and procedures complementing this Information Security Policy must also be properly communicated and made known to the persons, companies and institutions affected or involved in each case.

	Information Security Policy	09-09-2026 Page 9 of 22
Classification: Public	SGSI 01	Version 1.2

Communication, awareness and training programmes shall be defined periodically, and the rules on the use of information assets shall be made available to users.

Layers Of Reality will promote the necessary technical training in Information Security, especially for the Security and Systems Officers.

Access authorisation and control.

Access to information systems is controlled, monitored and limited to users, processes, devices and information systems with the minimum permitted and/or authorised functionalities.

The authorisations required for critical tasks shall be established and managed.

Protection of facilities.

Layers Of Reality systems and their communications infrastructure are located in duly protected areas, equipped with physical, redundancy, continuity and environmental security measures, and subject to a physical access control procedure.

Acquisition of security products and contracting of security services

When acquiring products, Layers Of Reality shall take into account that such products have certified security functionality related to the purpose of their acquisition, except where the proportionality requirements regarding the risks assumed do not justify it, in the opinion of the Security Officer.

The contracting of security services shall be governed by the preceding sections and by the provisions of the "Third parties" section later in this document.

Least Privilege and Security by Design.

At Layers Of Reality, systems are always designed and configured with Security by Default in mind. The system provides the minimum required functionality, as the operation, administration and activity logging functions are the minimum necessary, and Layers Of Reality ensures that they are only accessible to authorised persons and from authorised locations or equipment.

Functions that are unnecessary or inappropriate for the intended purpose shall be removed or disabled through configuration control. Ordinary use of the system must be simple and secure, so that insecure use requires a conscious act by the user. To this end, security configuration guides shall be applied for the different technologies, adapted to the system categorisation, in order to remove or disable unnecessary or inappropriate functions.

	Information Security Policy	09-09-2026 Page 10 of 22
Classification: Public	SGSI 01	Version 1.2

All projects related to or affecting information systems must include, in their analysis process, an assessment of the security requirements and define a security model agreed with the information security officer.

The concepts of security by design, secure coding and the applicable security controls and measures, according to the statement of applicability approved by Layers Of Reality, shall be taken into account and applied in the design, development, installation and management of information systems and in projects.

System integrity and updating.

At Layers Of Reality, systems are assessed periodically to know their security status at all times, taking into account manufacturers' specifications, vulnerabilities, configuration deficiencies, applicable updates and early incident detection, thereby managing their integrity.

All system components require authorisation prior to installation.

Protection of stored information and information in transit.

Information is classified according to the sensitivity required in its processing and the applicable security and protection levels.

Layers Of Reality pays particular attention to information stored or in transit through insecure environments. This includes information stored or processed on laptops, tablets, smartphones, peripheral devices and storage media, as well as communications over open networks or with weak encryption, where security measures are applied to ensure that information is handled in accordance with its classification.

Procedures shall be applied to ensure the long-term recovery and preservation of electronic documents produced by the information systems.

All information on non-electronic media that has been the cause or direct consequence of electronic information must be protected with the same degree of security as the latter. To this end, the measures appropriate to the nature of the medium shall be applied, in accordance with the applicable rules.

Protection against other interconnected information systems.

Layers Of Reality protects the access perimeter of its system, particularly connections via the Internet, always analysing the risks arising from interconnection with other systems and establishing measures that ensure the necessary level of security.

	Information Security Policy	09-09-2026 Page 11 of 22
Classification: Public	SGSI 01	Version 1.2

Activity logging and detection of malicious code

Layers Of Reality has enabled user activity logs that retain the information needed to monitor, analyse, investigate and document improper or unauthorised activities, making it possible to identify at any time the person acting. All of this with full guarantees of the right to honour, personal and family privacy and self-image of the persons concerned, and in accordance with personal data protection regulations and other applicable provisions.

Layers Of Reality implements a comprehensive process for detecting, reacting to and recovering from malicious code through procedures covering detection mechanisms, classification criteria, analysis and resolution procedures, as well as communication channels with stakeholders and the recording of actions taken.

In order to preserve the security of information systems, ensuring strict observance of the principles of action of public administrations, and in accordance with the General Data Protection Regulation and with respect for the principles of purpose limitation, data minimisation and storage limitation set out therein, incoming or outgoing communications may be analysed, to the extent strictly necessary and proportionate, and solely for information security purposes, so as to prevent unauthorised access to networks and information systems, stop denial-of-service attacks, and prevent the malicious distribution of malicious code and other damage to the aforementioned networks and information systems.

In order to correct or, where appropriate, demand accountability, every user accessing the information system must be uniquely identified, so that it is known at all times who receives access rights, what type of rights they are, and who has carried out a given activity.

Security incidents.

To prevent information and/or services from being harmed by security incidents, Layers Of Reality implements the established security measures, as well as any additional controls it has identified as necessary through a threat and risk assessment. These controls, as well as the security roles and responsibilities of all personnel, are clearly defined and documented.

When a significant deviation from the parameters pre-established as normal occurs, the necessary detection, analysis and reporting mechanisms shall be established so that they regularly reach those responsible.

Layers Of Reality shall establish the following measures for responding to security incidents:

- Mechanisms to respond effectively to security incidents.
- Designate a point of contact for communications regarding incidents detected in other departments or other bodies.

	Information Security Policy	09-09-2026 Page 12 of 22
Classification: Public	SGSI 01	Version 1.2

- Establish protocols for the exchange of information related to the incident. This includes two-way communications with Computer Emergency Response Teams.
- To ensure the availability of services, Layers Of Reality has the necessary means and techniques to guarantee the recovery of the most critical services.

Users have established channels to report immediately any incident or anomaly detected.

Business continuity.

Layers Of Reality makes the backups that ensure the recovery of information and establishes the appropriate mechanisms to guarantee continuity of operations in the event of loss of the usual means.

To this end, procedures have been developed to ensure the long-term recovery and preservation of the electronic documents and data produced within the scope of its competences.

Continuous improvement of the security process.

The security management system in place is continuously updated and improved, as required by the certifications and as described later in this document.

Legal Requirements and regulatory framework

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (GDPR).
- Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD).
- Royal Legislative Decree 1/1996 of 12 April, Intellectual Property Law.
- Law 2/2019 of 1 March amending the consolidated text of the Intellectual Property Law, approved by Royal Legislative Decree 1/1996 of 12 April, and transposing into Spanish law Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 and Directive (EU) 2017/1564 of the European Parliament and of the Council of 13 September 2017.
- Law 34/2002 of 11 July on information society services and electronic commerce.
- Royal Decree-Law 12/2018 of 7 September on the security of networks and information systems.

	Information Security Policy	09-09-2026 Page 13 of 22
Classification: Public	SGSI 01	Version 1.2

- Royal Decree 43/2021 of 26 January implementing Royal Decree-Law 12/2018 of 7 September on the security of networks and information systems.
- Royal Decree 311/2022 of 3 May regulating the National Security Scheme.
- Resolution of 13 October 2016 of the Secretary of State for Public Administrations approving the Technical Security Instruction on conformity with the National Security Scheme.
- Resolution of 7 October 2016 of the Secretary of State for Public Administrations approving the Technical Security Instruction on the Security Status Report.
- Resolution of 27 March 2018 of the Secretary of State for the Civil Service approving the Technical Security Instruction on the Security Audit of Information Systems.
- Resolution of 13 April 2018 of the Secretary of State for the Civil Service approving the Technical Security Instruction on the Notification of Security Incidents.
- UNE-ISO/IEC 27001:2023 Information security, cybersecurity and privacy protection. ISMS. Requirements.
- UNE-ISO/IEC 27002:2023 Information security, cybersecurity and privacy protection. Information security controls.

Likewise, the Security Officer shall be responsible for identifying the security guides of the National Cryptologic Centre (CCN) that will apply in order to improve compliance with the provisions of the National Security Scheme.

Roles, Responsibilities and Duties

Users

Any person or system accessing information processed, managed or owned by Layers Of Reality shall be considered a user. Users are responsible for their conduct when accessing information or using the IT systems of Layers Of Reality. Users are responsible for all actions carried out using their personal identifiers or credentials.

Users are obliged to:

- Comply with the Information Security Policy and complementary standards, procedures and instructions.
- Protect and safeguard the information of Layers Of Reality, preventing its disclosure, release outside the organisation, modification, deletion or

	Information Security Policy	09-09-2026 Page 14 of 22
Classification: Public	SGSI 01	Version 1.2

destruction, whether accidental or unauthorised, or its misuse, regardless of the medium or means through which it was accessed or became known.

- Know and apply the Information Security Policy, the Information Systems Rules of Use and all other applicable security policies, standards, procedures and measures.

Users who breach the Information Security Policy or the complementary standards and procedures may be sanctioned in accordance with the contracts governing their relationship with Layers Of Reality and with current applicable legislation.

Information Officer (National Security Scheme)

The Information Officer determines the requirements of the information processed and has the following responsibilities:

- Ensuring the proper use of the information and, therefore, its protection.
- Establishing the security requirements of the information.
- Determining the security levels of the information processed, assessing the consequences of a negative impact.

Service Officer (National Security Scheme)

The Service Officer shall have the following general responsibilities:

- Establishing the security requirements of the service, including interoperability, accessibility and availability requirements.
- Determining the security levels of the service, in agreement with the Security Officer and the System Officer.
- Maintaining the security of the information handled and of the services provided by the information systems within their area of responsibility.

Management

The management of Layers Of Reality is deeply committed to the policy described in this document and is aware of the value of information and of the serious economic and reputational impact that a security incident may cause.

In the context of the National Security Scheme, Management assumes the responsibilities described for the Information and Service Officers.

Management is therefore the owner of Layers Of Reality's information assets and is also responsible for the risks.

Management also assumes the following responsibilities:

	Information Security Policy	09-09-2026 Page 15 of 22
Classification: Public	SGSI 01	Version 1.2

- Demonstrating leadership and commitment with respect to the information security management system
- Ensuring that the information security policy and objectives are established and are compatible with the strategic direction of the organisation.
- Approving and communicating the Information Security Policy, the Information Systems Rules of Use and the importance of complying with them to all users, internal or external, customers and suppliers.
- Meeting and reaching agreements with the Corporate Security Committee and with the Security and Systems Officers, in order to be informed about the ISMS and update the Information Security strategy.
- Fostering a corporate information security culture.
- Supporting the continuous improvement of information security processes.
- Ensuring that the resources needed to comply with the information security policy and the systems rules of use, and to operate the information security management system, are available.
- Defining the approach to information security risk analysis and management and the criteria for accepting risks, and ensuring that risks are assessed at least annually.
- Ensuring that internal information security audits are carried out and that their results are reviewed to identify opportunities for improvement.
- Defining and controlling the information security budget.
- Approving training plans and improvements and projects related to Information Security.
- Approving documentation up to its second level of standards and procedures.
- Determining the measures, whether disciplinary or of any other kind, that may be applied to those responsible for security breaches.

Security Officer

The Security Officer takes the decisions needed to meet the security requirements of the information and services and supervises the implementation of the measures needed to ensure that the requirements are met, and shall report on these matters

The person holding the position of Information Security Officer shall assume the following functions:

	Information Security Policy	09-09-2026 Page 16 of 22
Classification: Public	SGSI 01	Version 1.2

- Promoting the security of the information handled and of the electronic services provided by the information systems, with the responsibility and authority to ensure that the Information Security Management System complies with the requirements of the National Security Scheme.
- Supervising compliance with this Policy, its standards, derived procedures and the security configuration of the systems.
- Establishing appropriate and effective security measures to meet the security requirements set by the Service and Information Officers, at all times following the requirements of Annex II of the ENS, and declaring the applicability of those measures.
- Promoting security awareness and training activities within their area of responsibility.
- Coordinating and monitoring the implementation of projects for alignment with the specified standards, in collaboration with the Systems Officer.
- Carrying out, with the collaboration of the System Officer, the mandatory risk analyses, selecting the safeguards to be implemented and reviewing the risk management process. Likewise, together with Management, accepting the residual risks calculated in that analysis.
- Promoting periodic audits to verify compliance with information security obligations and analysing the audit reports, drawing up the conclusions to be presented to the System Officer so that the appropriate corrective measures can be adopted.
- Coordinating the Security Management process, in collaboration with the Systems Officer.
- Signing the Statement of Applicability, which comprises the list of security measures selected for a system.
- Preparing periodic security reports including the most relevant incidents in each period, in coordination with the Systems Officer.
- Determining the category of the system according to the procedure described in Annex I of the ENS and the security measures to be applied in accordance with Annex II of the ENS.
- Verifying that the security measures are adequate for the protection of information and services.
- Preparing the items to be discussed at Security Committee meetings, in coordination with the System Officer, providing timely information for decision-making.
- Responsible for the direct or delegated execution of Management decisions, the Security Officer shall meet with Management and with the System Officer to ensure the strategy is implemented.

	Information Security Policy	09-09-2026 Page 17 of 22
Classification: Public	SGSI 01	Version 1.2

With regard to documentation, and with the support of the System Officer, the functions of the Security Officer are:

- Proposing to Management, the Security Committee and the Systems Officer, for approval, the second-level security documentation (ICT Security Standards –STIC– and General Procedures of the Information Security Management System –ISMS–) and signing such documentation.
- Approving third-level security documentation (STIC Operating Procedures and STIC Technical Instructions).
- Keeping documentation organised and up to date, managing the mechanisms for accessing it.

In performing any of their functions, the Security Officer may request the collaboration of the System Officer.

Data Protection Officer

In accordance with the GDPR and the LOPDGDD, the Data Protection Officer shall have at least the following functions:

- Informing and advising data controllers and, in general, the organisation's personnel of their obligations under the GDPR and other data protection provisions.
- Monitoring compliance with the Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- Providing advice where requested as regards the data protection impact assessment and monitoring its performance pursuant to Article 35 of the GDPR;
- Cooperating with the supervisory authority;
- Acting as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 of the GDPR, and consulting, where appropriate, with regard to any other matter.

System Officer

The System Officer, directly or through in-house or contracted resources, is responsible for developing the specific way in which security is implemented in the system and for supervising its day-to-day operation, and may delegate to administrators or operators under their responsibility.

	Information Security Policy	09-09-2026 Page 18 of 22
Classification: Public	SGSI 01	Version 1.2

The functions of the System Officer shall be as follows:

- Developing, operating and maintaining the Information system throughout its life cycle, including its specifications, installation and verification of its correct operation.
- Defining the topology and management system of the Information System, establishing the criteria for use and the services available in it.
- Ensuring that specific security measures are properly integrated within the general security framework.
- Carrying out exercises and tests on existing security operating procedures and continuity plans.
- Monitoring the life cycle of systems: specification, architecture, development, operation, changes.
- Implementing the measures needed to guarantee system security throughout its life cycle, in agreement with the Security Officer.
- Approving any substantial change to the configuration of any system component.
- Carrying out, with the collaboration of the Security Officer, the mandatory risk analyses, selecting the safeguards to be implemented and reviewing the risk management process.
- Preparing, in collaboration with the Security Officer, third-level security documentation (STIC Operating Procedures and STIC Technical Instructions).

System Security Administrator

Their functions shall be as follows:

- Implementing, managing and maintaining the security measures applicable to the information system.
- Managing, configuring and updating, where appropriate, the hardware and software on which the security mechanisms and services of the information systems are based.
- Managing the authorisations granted to system users, in particular the privileges granted, including monitoring that the activity carried out in the system conforms to what has been authorised.
- Applying security operating procedures.
- Applying configuration changes to the information system.

	Information Security Policy	09-09-2026 Page 19 of 22
Classification: Public	SGSI 01	Version 1.2

- Ensuring that the established security controls are strictly complied with, and that the approved procedures for operating the information system are applied.
- Supervising hardware and software installations, modifications and upgrades to ensure that security is not compromised and that they comply with the relevant authorisations at all times.
- Monitoring the security status of the system as reported by the security event management tools and technical audit mechanisms implemented in the system.
- Informing those responsible of any security-related anomaly, compromise or vulnerability.
- Collaborating in the investigation and resolution of security incidents, from detection to resolution.

Information Security Committee

Made up of the Corporate Managing Director, the Managing Director of Media, the Director of the Legal Department, the Director of Information Technology and the Information Security Officer, the Committee meets periodically to coordinate information security across the organisation.

Its functions are as follows:

- Responding to requests on Information Security matters from the Administration and from the various security roles and/or areas, reporting regularly on the status of Information Security.
- Providing advice on Information Security matters.
- Resolving conflicts of responsibility that may arise between the different administrative units.
- Promoting the continuous improvement of the Information Security management system. To this end, it shall be responsible for:
 - Coordinating the efforts of the different areas in Information Security matters, to ensure that they are consistent and aligned with the strategy decided in this area, and avoiding duplication.
 - Proposing Information Security improvement plans, with the corresponding budget allocation, prioritising security actions when resources are limited.
 - Ensuring that Information Security is taken into account in all projects from their initial specification to their entry into operation. In particular, it shall ensure the creation and use of horizontal

	Information Security Policy	09-09-2026 Page 20 of 22
Classification: Public	SGSI 01	Version 1.2

services that reduce duplication and support the homogeneous operation of all ICT systems.

- Monitoring the main residual risks assumed and recommending possible actions in respect of them.
- Monitoring the management of security incidents and recommending possible actions in respect of them.
- Regularly reviewing this Information Security Policy for approval by the competent body.
- Drawing up the Information Security regulations for approval in coordination with General Management.
- Verifying the information security procedures and other documentation for approval.
- Drawing up training programmes aimed at training and raising staff awareness of Information Security and personal data protection.
- Drawing up and approving the training and qualification requirements for administrators, operators and users from an Information Security perspective.
- Promoting the periodic ENS and data protection audits that make it possible to verify compliance with the organisation's information security obligations.

Appointment and conflict resolution procedure

The Information Security Committee of Layers Of Reality **assigns, renews and communicates** the responsibilities, authorities and roles relating to information security, determining in each case the reasons and the period of validity. It shall also ensure that users know, accept and exercise the responsibilities, authorities and roles assigned, **resolving any conflicts** that arise in relation to each Information Security responsibility.

The Security Officer shall be a different person from the System Officer, and there shall be no hierarchical dependency between them.

Personal Data

The organisation shall only collect personal data when they are adequate, relevant and not excessive in relation to the scope and purposes for which they were obtained. Likewise, it shall adopt the technical and organisational measures necessary to comply with the Data Protection regulations in force at any given time.

	Information Security Policy	09-09-2026 Page 21 of 22
Classification: Public	SGSI 01	Version 1.2

Accordingly, under the LOPDGDD the appropriate measures have been adopted, such as the analysis of the legal basis of each data processing operation carried out, risk analysis, impact assessment where the risk is high, the record of processing activities and the appointment of the person who will perform the functions of Data Protection Officer.

Third parties

When the organisation provides services to other bodies, or handles information from other bodies, they shall be made aware of this Information Security Policy. Layers Of Reality shall define and approve the channels for coordinating information and the procedures for responding to security incidents, as well as any other actions that Layers Of Reality carries out in Security matters in relation to other bodies.

When Layers Of Reality uses third-party services or transfers information to third parties, they shall be made aware of this Security Policy and of the existing Security Regulations applicable to those services or that information. Such third party shall be subject to the obligations set out in those regulations and may develop its own operating procedures to comply with them. Specific procedures for communicating and resolving incidents shall be established. It shall be ensured that third-party personnel are adequately aware of security, at least to the same level as established in this Security Policy.

When any aspect of this Security Policy cannot be met by a third party as required in the preceding paragraphs, a report from the Security Officer shall be required specifying the risks incurred and how they are to be treated. This report must be approved by those responsible for the information and services affected before proceeding.

Third parties as outsourced Security services

In the case of outsourced services, except for justified and documented reasons, the organisation providing those services must designate a POC (Point or Person of Contact) for the security of the information processed and the service provided, who has the support of the management bodies and who channels and supervises both compliance with the security requirements of the service provided or solution supplied and communications relating to information security and incident management within the scope of that service.

Said security POC shall be the Security Officer of the contracted organisation, shall form part of its area, or shall have direct communication with it.

	Information Security Policy	09-09-2026 Page 22 of 22
Classification: Public	SGSI 01	Version 1.2

ISMS Development, Review and Audits

The Information Security Committee has approved the development of an information security management system (ISMS) that is established, implemented, maintained and improved in accordance with security standards. This system shall be adapted to and serve to manage the controls of the National Security Scheme. The system shall be documented and shall make it possible to generate evidence of the controls and of the achievement of the objectives set. There is a document management procedure that establishes the guidelines for structuring the system's security documentation, its management and access.

The Information Security Policy and Standards shall be adapted to the evolution of systems and technology and to organisational changes, and shall be aligned with current legislation and with the standards and best practices of the National Security Scheme, paying particular attention to the guides published by the National Cryptologic Centre as a development of the security measures and controls.

The applicable security measures and physical, administrative and technical controls shall be detailed in the Statement of Applicability, and shall be proportionate to the criticality of the information to be protected and to its classification.

The Information Security Committee shall review this policy annually or when significant changes so advise, and shall resubmit it for approval by management. Reviews shall verify the effectiveness of the policy, assessing the effects of technological and business changes.

Management shall be responsible for approving the necessary amendments to the text when a change occurs that affects the risk situations established in this document.

The security management system shall be audited annually, according to an audit plan drawn up by the security officer.