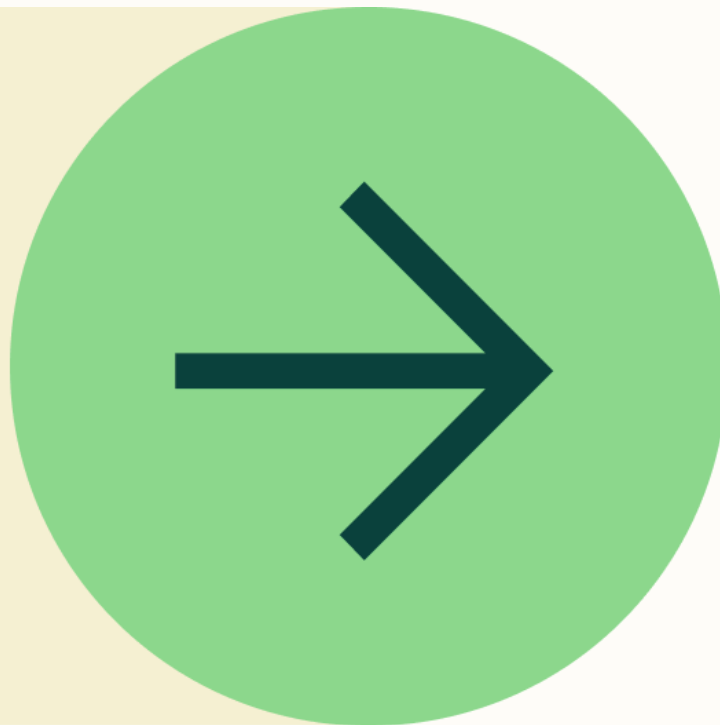


Security Policy



© 2023 All Right reserved.

This document is labeled as Public and has limited access.

It can not be distributed without prior authorization from Sales Layer Tech S.L.

	Developed by	Approved by
Name	Eduardo Fernández	Alvaro Verdoy
Role	Security Manager	CEO
Date	Apr 15, 2026	Apr 15, 2026

History Version

Version	Date	Comment
33	Apr 15, 2026	Normative references updated to UNE-EN ISO/IEC 27001:2023, ISO/IEC 27002:2022. Scope updated to include context and exclusions statement. Mission and Leadership sections revised. ISMS objectives, risk management and roles updated for alignment with current certification standard.
32	Apr 3, 2025	Mission, Commitment and Leadership updated. Terms and Definitions updated. Risk Management updated.
31	Apr 15, 2024	Functions and responsibilities, normative references, and the rest of the document reviewed and updated.

This table shows the last 3 versions of the document. Full version history is available in the document control system upon request.

Indice

Indice	4
Overview	5
Terms and definitions	6
Scope	8
Mission, Commitment and Leadership	8
Normative references	9
ISMS Security Objectives	10
Risk Management	11
Risk Assessment Process	11
Risk Treatment and Control Selection	12
Monitoring and Continuous Improvement	12
Development of the Information Security Policy	13

Overview

SALES LAYER TECH S.L. including all its subsidiaries (Sales Layer, Ltd. and Sales Layer, Inc.), hereinafter, referred to as **SALES LAYER, COMPANY or ORGANIZATION**, depends on ICT (Information and Communications Technology) systems to achieve its objectives. These systems must be managed with diligence, taking the appropriate measures to protect them against accidental or deliberate damage that may affect the availability, integrity or confidentiality of the information processed or the services provided.

To defend against these threats, a strategy that adapts to changes in environmental conditions is required to ensure the continuous provision of services. This implies that the company must apply the minimum security measures required by regulations, standards and other stakeholders, in addition to others derived from the risk analysis, as well as carry out continuous monitoring of the levels of service provision, monitor and analyze the reported vulnerabilities, and prepare an effective response to the incidents to guarantee the continuity of the services provided.

The different departments must ensure that ICT security is an integral part of each stage of the system's life cycle, from conception to decommissioning, through development or acquisition decisions and operational activities. Security requirements and financing needs must be identified and included in planning, request for proposals, and bidding documents for ICT projects.

Departments must be prepared to prevent, detect, react and recover from incidents, in accordance with security regulations.

Prevention

The company must avoid, or at least prevent as much as possible, information or services from being harmed by security incidents. For this, the departments must implement the appropriate security measures determined by regulations, standards and other stakeholders, as well as any additional control identified through an evaluation of threats and risks. These controls and security roles and responsibilities of all personnel, should be clearly defined and documented.

To ensure compliance with the policy, departments must:

- Authorize the systems before going into operation.
- Regularly assess security, including assessments of configuration changes

made routinely.

- Request periodic review by third parties in order to obtain an independent evaluation.

Detection

Given that services can be quickly degraded due to incidents, ranging from a simple slowdown to a stoppage, services must continuously monitor the operation to detect anomalies in the levels of service provision and act accordingly as established in control over the review of information security policies.

Monitoring is especially relevant when lines of defense are established. Detection, analysis and reporting mechanisms will be established regularly for those who are responsible to detect when there are significant deviations from the parameters that have been pre-established as normal.

Response

The organization must:

- Establish mechanisms to respond effectively to security incidents.
- Designate a point of contact for communications regarding incidents detected in third parties to whom it provides services.
- Establish protocols for the exchange of information related to the incident. This includes communications, in both directions, with the security incident response center (INCIBE-CERT).

Recovery

To ensure the availability of essential services, the security and technology departments formulate continuity plans for ICT systems. These plans should be an integral component of their overall business continuity strategy and disaster recovery plan.

Terms and definitions

The following terms are relevant to this policy and aligned with ISO/IEC 27000 and ISO/IEC 27005 standards, as well as other applicable regulatory frameworks. All defined terms should be interpreted consistently throughout the organization.

- **Asset:** Anything that has value to the organization and is related to the processing or storage of information. This includes systems, data, media, infrastructure, buildings, personnel, and more.
- **Availability:** The property of being accessible and usable upon demand by an authorized entity (person, system, or process).
- **Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Control:** A measure that is modifying risk. Controls include any process, policy, device, practice, or other actions which modify risk
- **Event (Security Event):** An identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may lead to an incident.
- **Information Security Incident:** A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations or information security.
- **Information Security Management System (ISMS):** A set of interrelated or interacting elements (organizational structure, policies, planning activities, responsibilities, processes, and resources) used to establish, implement, operate, monitor, review, maintain, and improve information security, based on risk management and continuous improvement principles.
- **Integrity:** The property of safeguarding the accuracy and completeness of assets (especially data), ensuring they are not modified in an unauthorized or undetected way.
- **Policy (Security Policy):** A formal statement from management that defines the principles, rules, and requirements for protecting the organization's information assets.
- **Residual Risk:** The risk that remains after risk treatment has been applied.
- **Risk:** The potential that a given threat will exploit a vulnerability to cause harm to an asset. Usually expressed as a combination of the probability of an event and its consequences.
- **Risk Management:** Coordinated activities to direct and control an organization with regard to risk, including identifying, analyzing, evaluating, and treating risk.
- **Risk Treatment:** The process of selecting and implementing measures to modify risk, which may include avoiding, optimizing, transferring, or accepting it.
- **Stakeholder:** A person or group that has an interest in any decision or activity of the organization.
- **System (Information System):** A set of interrelated components that collect, process, store, and distribute information, supporting decision-making and control in an organization.
- **Threat:** A potential cause of an unwanted incident that may result in harm to a system, service, or the organization.
- **Vulnerability:** A weakness in an asset or group of assets that can be exploited by one or more threats.
- **Statement of Applicability (SoA):** A documented statement describing the information security controls that are applicable to the organization's ISMS,

including justification for their inclusion or exclusion, and their implementation status.

- **Third Party:** Any external individual, organization, or supplier that has access to, processes, or handles the organization's information assets or systems under a contractual or service relationship.

Scope

This policy applies to all business processes of SALES LAYER TECH S.L, including all its subsidiaries (SALES LAYER, Ltd. and SALES LAYER, Inc.), as well as employees, contractors and third parties who have access to the company's information systems. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

The scope has been defined taking into account the internal and external context of the organization and the requirements of relevant interested parties, in accordance with UNE-EN ISO/IEC 27001:2023.

No exclusions are made from the scope of the ISMS.

Mission, Commitment and Leadership

Sales Layer's business mission is to enable marketing teams globally to create superior shopping experiences in both business-to-business and direct-to-consumer channels.

In support of this mission, SALES LAYER is committed to protecting its information assets and those of its stakeholders by establishing, maintaining, and continuously improving an Information Security Management System (ISMS) in accordance with UNE-EN ISO/IEC 27001:2023.

Top management:

- Ensures that the information security strategy is aligned with the organization's overall business objectives.
- Provides the necessary resources (human, technical, and financial) to implement and maintain the ISMS.
- Defines and approves the information security policy and promotes a culture of information security across all areas of the organization.

- Reviews and approves this Information Security Policy at least annually or upon significant changes to the organization, its context, or the threat landscape.
- Communicates the importance of effective information security management and compliance with ISMS requirements.
- Ensures that legal, regulatory, and contractual obligations related to information security are identified and fulfilled.
- Establishes measurable information security objectives and reviews them regularly.
- Promotes continual improvement of the ISMS through monitoring, evaluation, and corrective actions.
- Establishes a cross-functional Information Security Committee to coordinate and oversee security initiatives and compliance efforts.
- Ensures that information security is considered in all business processes and decision-making at every level.

Normative references

SALES LAYER is subject, by way of example and not limitation, to the following laws, standards and regulations:

International Standards

- UNE-EN ISO/IEC 27001:2023 – Information Security Management Systems – Requirements
- ISO/IEC 27002:2022 – Information security controls
- ISO/IEC 27005:2022 – Information Security Risk Management

European Legislation

- Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, regarding the protection of natural persons with regard to the processing of personal data and the free circulation of these data and by which repeals Directive 95/46/EC (General Data Protection Regulation)
- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Directive (EU) 2022/2555 of the European Parliament and of the Council of

14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Spanish Legislation

- Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights
- Law 34/2002 (LSSI-CE), of July 11 – Information Society Services and Electronic Commerce
- Royal Legislative Decree 1/1996 – Intellectual Property Law
- Law 10/2010, of April 28, on the prevention of money laundering and the financing of terrorism

Other Jurisdictional Regulations

- California Consumer Privacy Act (CCPA)
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)
- Computer Fraud and Abuse Act (CFAA)
- Data Protection Act 2018 (UK DPA) – UK national law complementing GDPR, applicable to processing of personal data in the UK.

ISMS Security Objectives

This policy demonstrates the commitment of senior management and has the following objectives:

- **Ensure Legal and Regulatory, and Standard Compliance:** Comply with all applicable legal, regulatory, contractual, and normative requirements related to information security and data protection, including recognized standards such as ISO/IEC 27001 and other industry-specific frameworks adopted by the organization
- **Preserve Confidentiality, Integrity, and Availability (CIA):** Safeguard the organization's information assets by ensuring their confidentiality, integrity, and availability at all times.
- **Promote a Security-Aware Culture:** Foster an organizational culture where all employees understand and actively participate in protecting information through awareness and regular training programs.
- **Manage Third-Party Security Risks:** Ensure that all suppliers, contractors, and third parties comply with the organization's security policies and

undergo appropriate risk assessments.

- **Maintain an Effective Risk Management Framework:** Conduct risk assessments regularly and whenever significant changes occur, implement appropriate treatment plans, and continuously monitor the risk landscape.
- **Measure Performance and Promote Continuous Improvement:** Establish mechanisms to measure the effectiveness of the ISMS and related controls. Use performance evaluation, internal audits, incident analysis, and stakeholder feedback to drive continual improvement of the system.
- **Ensure Business Continuity and Resilience:** Develop, implement, and test business continuity and disaster recovery plans to maintain operations during disruptions and recover information systems within acceptable timeframes.
- **Align Information Security with Business Strategy:** Ensure that information security objectives are consistent with and support the organization's strategic goals and digital initiatives.

The measurable targets, key performance indicators (KPIs), responsible parties, and timelines associated with each of the above objectives are defined, monitored, and reviewed as part of the annual ISMS Management Review process, in accordance with UNE-EN ISO/IEC 27001:2023. Results are documented in the corresponding Management Review records.

Risk Management

SALES LAYER considers risk management a fundamental pillar of its Information Security Management System (ISMS). A documented risk management methodology has been established to ensure that the organization can achieve expected outcomes, minimize potential disruptions, and support continual improvement.

Risk Assessment Process

Risk assessments are carried out under the following circumstances:

- At least once a year as part of the ISMS review cycle.
- When there are significant changes in the organization's systems, services, processes, or external environment.
- Following major security incidents or the identification of critical vulnerabilities.
- During the launch of new projects or the adoption of emerging technologies.

The assessment process includes:

- Identification of assets, threats, vulnerabilities, and their potential impact.
- Estimation of the likelihood of occurrence and the impact severity.
- Evaluation of the level of risk and comparison with predefined acceptance criteria.
- Classification and prioritization of risks based on business impact.

Risk assessment methodology are defined and documented in the Risk Management Procedure, in accordance with ISO/IEC 27005:2022.

Risk Treatment and Control Selection

Based on the results of the assessment, a Risk Treatment Plan is developed to reduce, transfer, accept, or avoid identified risks. Security controls are selected primarily from ISO/IEC 27002:2022, which comprises 93 controls organized across four domains: Organizational, People, Physical, and Technological controls, as well as from other relevant standards when applicable.

All control decisions are documented in the Statement of Applicability (SoA), which justifies the inclusion, exclusion, and implementation status of each control.

Residual risks that exceed the acceptable thresholds must be formally reviewed by senior management.

Monitoring and Continuous Improvement

The risk environment is continuously monitored through vulnerability reports, incident reviews, internal audits, and external changes. Risk assessments are updated accordingly to reflect current exposure and ensure that controls remain effective.

The entire risk management process supports the organization's goal of continual improvement of the ISMS.

Development of the Information Security Policy

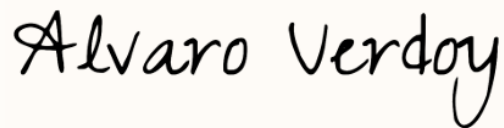
The Security Manager is responsible for reviewing and updating this Security Policy at least annually or whenever significant changes occur in the organization, its context, regulatory requirements, or following major security incidents. The Policy will be approved by the CEO of SALES LAYER and disseminated for the knowledge of all stakeholders.

This policy is distributed to all employees via the internal documentation portal. All new employees are required to read and acknowledge this policy as part of their onboarding process. Awareness of the policy is reinforced periodically through mandatory training and internal communications.

Additionally, the policy is made available to all relevant external stakeholders through the company's website or upon request.

Valencia,

2026-04-15

A handwritten signature in black ink that reads "Alvaro Verdoy".

Alvaro Verdoy

CEO SALES LAYER