Security Policy

sales layer

	Developed by	Approved by
Name	Eduardo Fernández	Álvaro Verdoy
Role	Security Officer	CEO
Date	02/02/2023	02/02/2023

History Version

Version	Date	Comment
31	Feb 02, 2023 13:56	Including all Sales Layer subsidiaries
28	Jan 30, 2023 15:09	Minor changes in the document
26	Jan 25, 2023 15:40	Minor changes in roles and risk management
24	Jan 24, 2023 13:56	Risk management updated
21	Jan 20, 2023 13:22	Revised and summarized.
1	Sep 29, 2021 15:02	Document created

Security Policy **0**

Overview 3

Prevention 3

Detection 4

Response 4

Recovery 4

Scope 4

Mission, Commitment and Leadership 4

ISMS Security Objectives 5

Risk Management 5

Development of the Information Security Policy 6

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 minimum 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 critical services, departments should develop ICT system continuity plans as part of their overall plan for business continuity and recovery plan.

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.

Mission, Commitment and Leadership

The company's mission is to enable marketing teams globally to create superior shopping experiences in both the business to business and direct to consumer channels.

Senior Management of SALES LAYER undertakes to facilitate and provide the necessary resources for the establishment, implementation, maintenance and improvement of the Information Security Management System, as well as to demonstrate leadership and commitment with respect to it, through the constitution of the Security Committee, of their roles and responsibilities.

ISMS Security Objectives

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

- Ensure compliance with applicable laws, regulations and standards.
- Comply with stakeholder security requirements.
- Adopt the principle of safety by default and apply safety as a holistic process.
- Preserve the confidentiality, integrity and availability of the information across all company assets.
- Create a security awareness plan that allows employees to be aware of the risks to which the organization is exposed.
- Provide senior management leadership to ensure that security objectives are established and aligned with business strategy.
- Assign general and specific information security responsibilities for defined roles.
- Establish a continuous improvement system to address any deviations, new risks, or changes in regulatory or information security requirements.
- Periodically review the ISMS documentation to adapt it to new security requirements or risks.
- Ensure that a risk analysis is performed at least annually or when new emerging threats arise , develop a treatment plan, apply all necessary controls and monitor risks.
- Establish procedures for the prevention, detection, response and recovery of information in the event of a security incident.

Risk Management

SALES LAYER knows that risk management is a critical component of its operations and that it ensures that its resources and stakeholders' data is protected. SALES LAYER has defined a risk management procedure with the objective of ensuring that the Information Security Management System can achieve expected results, prevent and reduce undesired effects and achieve continuous improvement.

This analysis will be repeated:

- Regularly, at least once a year.
- When the information handled and/or the services provided change significantly, including new risks.
- When a serious security incident occurs or serious vulnerabilities are detected.
- When exist new projects or implementations of new or emerging technologies

SALES LAYER identifies all threats to which assets are exposed, the impact they may have if they materialize and the likelihood of recurrence. Based on this data, the organization performs an analysis of the potential risk and generates a Risk Treatment Plan to take action on its mitigation, acceptance, elimination or transfer.

The results of the risk management process are constantly documented, monitored and reviewed by the Security Committee.

Development of the Information Security Policy

The Security Officer is responsible for reviewing and updating this Security Policy at least annually. The Policy will be approved by the CEO of SALES LAYER and disseminated for the knowledge of all the stakeholders.

This Policy will be developed through security regulations that address specific aspects. The security regulations will be available to all members of the organization who need to know them, particularly those who use, operate or manage the information and communications systems.

Valencia, Feb 2, 2023

Álvaro Verdoy

CEO SALES LAYER