NEARBY COMPUTING

Information Security Policy

Nearby Computing

NearbyOne and other trademarks and designs are the registered or unregistered trademarks of Nearby Computing SL. and its subsidiaries in the Spain and in foreign countries. All other trademarks are the property of their respective owners. The Nearby Computing SL. trademarks may not be used in connection with any product or service that is not Nearby Computing's in any manner that is likely to cause confusion among customers or in any manner that disparages or discredits Nearby Computing SL.
This document contains information that is the property of Nearby Computing SL. This document may not be copied, reproduced, reduced to any electronic medium or machine-readable form, or otherwise duplicated, and the information herein may not be used, disseminated, or otherwise disclosed, except with the prior written consent of Nearby Computing SL.

Copyright© 2025 Nearby Computing SL. All Rights Reserved

VERSION	DATE	REASON
1.0	17/03/2025	Document creation
1.1	01/09/2025	Integration of ENS and ISMS Information Security Management System (ISO/IEC 27001)

PREPARED BY	REVIEWED BY	APPROVED BY
ISMS Manager	CISO	CEO

© Nearby Computing 2025 | Public

1 Contents

© Nearby Computing 2025 | Public

2 Purpose &Scope

Nearby Computing has decided to implement an Information Security Management System (ISMS) based on ISO/IEC 27001, aligned with the requirements of the National Security Framework (High Level). This comprehensive approach aims to achieve the following objectives:

- Ensure the confidentiality, availability, integrity, authenticity, and traceability of information, both in the products and services offered to clients and in internal management.
- Comply with legal, regulatory, and client requirements related to information security, while also providing added value in the delivery of products and services, addressing information security needs throughout their entire lifecycle.
- Inspire trust among all organizations and individuals who interact with Nearby Computing.
- Define clear responsibilities for fulfilling the various tasks and obligations associated with information security.
- Follow the process of continuous improvement.
- Ensure compliance with applicable standards, laws, and regulations from a security perspective, with particular attention to Security, Data Protection, Labor Rights, and Intellectual Property.

Special emphasis will be placed on raising awareness among all personnel involved in the process, as well as their direct supervisors, so that neither ignorance, lack of organization and coordination, nor inadequate instructions become sources of security risk.

The goal of information security is to guarantee the quality of information and the continuous delivery of services by acting preventively, monitoring daily operations, and responding promptly to security incidents.

This document defines the information security policy of Nearby Computing and applies to all stakeholders and information assets of Nearby Computing.

3 Development

Nearby Computing depends on information transmission and processing assets to achieve its objectives. These systems must be managed diligently, taking appropriate measures to protect them against accidental or deliberate damage that could affect the **availability,**

© Nearby Computing 2025 | Public

integrity, confidentiality, authenticity, and traceability of the information processed or the services provided.

3.1 Prevention

Individuals must avoid, or at least prevent to the greatest extent possible, information or services are compromised by information security incidents.

To this end, Nearby Computing must implement the minimum information security measures determined by the ENS, as well as any additional controls identified through a threat and risk assessment. These controls, and the information security roles and responsibilities of all individuals, must be clearly defined and documented.

To ensure compliance with the policy, Nearby Computing must:

- Authorize information assets before they go into operation.
- Regularly assess information security, including evaluations of routine configuration changes.
- Request periodic reviews by third parties to obtain an independent assessment.

3.2 Detection

Since services and assets can quickly deteriorate due to information security incidents, ranging from a simple slowdown to a complete shutdown, operations must be continuously monitored to detect anomalies in service performance levels and act accordingly.

Monitoring is especially relevant when lines of defense are established.

Mechanisms for detection, analysis, and reporting have been established, which regularly reach those responsible and whenever a significant deviation occurs from parameters predefined as normal.

3.3 Response

Nearby Computing has:

- Established mechanisms to effectively respond to information security incidents.
- Designated a point of contact for communications regarding detected information security incidents.
- Established protocols for the exchange of information related to incidents.

© Nearby Computing 2025 | Public

3.4 Recovery

To ensure the availability of critical services, Nearby Computing has developed service continuity plans as part of its overall business continuity and recovery activities.

4 Regulatory Framework

Nearby Computing is subject to the following laws, regulations, and other national and international standards on information security:

- ISO/IEC 27001 Information Security Management System (certification obtained by Nearby Computing).
- Royal Decree 311/2022, of May 3, regulating the National Security Framework (ENS).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation – GDPR).
- Organic Law 3/2018, of December 5, on Personal Data Protection and the guarantee of digital rights.
- Royal Decree 1720/2007, of December 21, approving the Regulation implementing Organic Law 15/1999 (still in force for articles not in contradiction with the GDPR).
- Law 34/2002, of July 11, on Information Society Services and Electronic Commerce.
- Royal Legislative Decree 1/1996, of April 12, approving the revised text of the Intellectual Property Law.

4.1 Information Security Organization

At Nearby Computing, the governance of information security is structured to ensure compliance with the Esquema Nacional de Seguridad (ENS) and other applicable legal and regulatory frameworks. The following roles and responsibilities are defined:

4.1.1 Information Security Committee

The Information Security Committee is the highest authority in the organization regarding information security. It is responsible for coordinating compliance with customer requirements, legal obligations, and regulatory standards, including ENS. It also manages potential conflicts related to information security. The committee is composed of the Chief Information Security Officer (CISO), Chief Technology Officer (CTO), ISMS Manager, Product Manager, and Site Reliability Engineer.

© Nearby Computing 2025 | Public

4.1.2 Chief Information Security Officer (CISO)

The CISO serves as the primary security officer and is responsible for defining the protection levels and security controls for organizational assets, based on their classification and criticality. This role is held by the Director of Engineering and Operations, ensuring alignment with ENS requirements for asset protection and risk management.

4.1.3 Department Directors

Each department director is accountable for the information managed within their respective areas. When external systems are used to process or store data, the department director also assumes the role of system owner. This responsibility may be delegated to other team members for specific systems, ensuring that accountability remains clearly defined.

4.1.4 System Classification and Conflict Resolution

The CISO initiates the classification of systems and data, proposing protection levels based on defined criteria aligned with ENS classification levels. These classifications are reviewed and approved by the respective information owners. Any conflicts or discrepancies are escalated to the Information Security Committee, which resolves them and communicates decisions to the Steering Committee, ensuring transparency and traceability.

4.1.5 Service responsible

In alignment with ENS role definitions, the following individuals are designated as service owners for key operational areas:

- Design and Software Development: Chief Technology Officer (CTO)
- Professional Services: Director of Engineering and Operations
- Maintenance and Support: Director of Engineering and Operations

4.1.6 Point of Contact

The Point of Contact (POC) of Nearby Computing is the email address cybersecurity@nearbycomputing.com

4.2 Review, Approval and Communication of the Information Security Policy

The Information Security Committee approves the information security policy, reviews it at least annually, and communicates it to the Board of Directors of Nearby Computing.

The information security policy is published on the corporate website

© Nearby Computing 2025 | Public

4.3 Personal Data

Nearby Computing processes personal data in compliance with current personal data protection legislation.

4.4 Information Security Risk Analysis and Management

A risk analysis has been carried out for all information assets of Nearby Computing, evaluating the threats and risks to which they are exposed.

This analysis is reviewed and, if necessary, updated:

- Regularly, at least once a year.
- When the information handled changes.
- When the services provided change.
- When a serious information security incident occurs.
- When serious vulnerabilities are reported.

4.5 Development of the Information Security Policy

This information security policy is further developed in other, more specific policies, regulations, and procedures.

4.6 Obligations of Personnel

All personnel, both internal and subcontracted, of Nearby Computing are required to be aware of and comply with this information security policy and the other documents that develop it.

All personnel are regularly made aware, particularly new hires.

Personnel responsible for the use, operation, or administration of information systems will receive training for the secure management of systems to the extent needed to perform their work. Training is mandatory before assuming any responsibility, whether it is their first assignment or a change in job position or responsibilities.

4.7 Third Parties

When Nearby Computing provides services or processes information from other organizations:

They are made aware of this information security policy.

Reporting and coordination channels are established with the Information Security Committee.

© Nearby Computing 2025 | Public

Procedures are established for responding to information security incidents.

When Nearby Computing uses third-party services or transfers information to third parties:

They are made aware of this policy and of the information security regulations applicable to such services or information.

The third party is subject to the obligations set forth in such regulations and may develop its own operating procedures to comply with them.

Specific procedures for incident reporting and resolution are established.

It is required that third-party personnel are adequately trained in information security, at least to the level set in this policy.

When any aspect of the policy cannot be met by a third party as required in the previous paragraphs, a report from the CISO is required to specify the risks incurred and how to address them. This report must be approved by the Information and Service Owners concerned before proceeding.

© Nearby Computing 2025 | Public