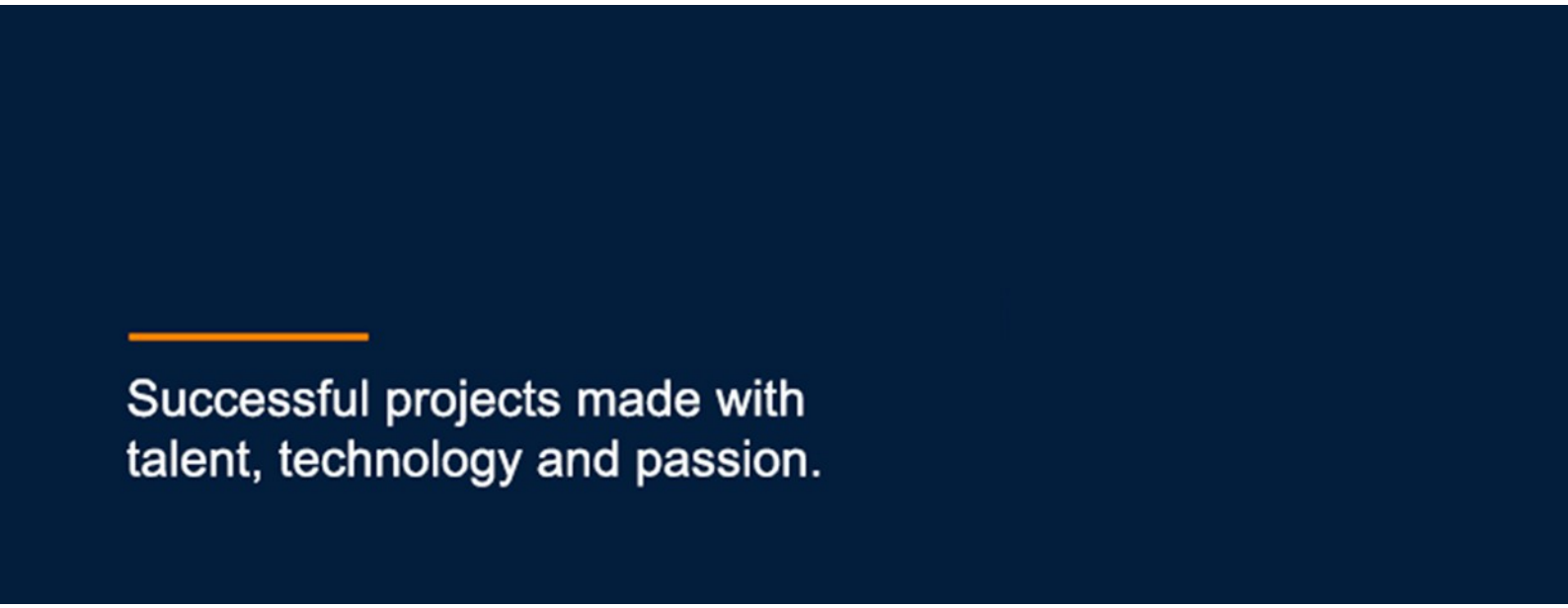
netboss®
COMUNICACIONES



SGSI D51 01 Information Security Policy

Santander (ES), January 29, 2026 Version:
1.10

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es

Version Control

Version control			
Date	Author	Version	Changes
12/29/2017	Management Systems Department	1.0	Initial version
02/08/2019	Management Systems Directorate	1.1	Update to sections 1.8, 2.5, 3.2, and 3.3
July 5, 2019	Management Systems Department	1.2	Update to section 3.1
09/16/2019	Management Systems Department	1.3	Format update
July 23, 2020	Management Systems Division	1.4	Update to section 3.1 and organizational chart
March 4, 2021	Management Systems Department	1.5	Organizational chart update
February 22, 2022	Management Systems Division	1.6	Update and revision
09/08/2022	Administration Department	1.7	Update to section 3.1
02/27/2024	Management Systems Division	1.8	Update to organizational chart and section 9.8
January 22, 2025	Management Systems Department	1.9	Update on legislation and other matters
January 29, 2026	Management Systems Department	1.10	Update to Section 5
Document reviewed and approved by management - Valid without signature			

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es

CONTENTS

1. Introduction 6
1.1. Presentation of the Organization 6
1.2. Importance of ICT Systems and Information Security 6
1.3. General Concepts 7
1.4. Prevention 8
1.5. Detection 8
1.6. Response 8
1.7. Recovery 9
1.8. Applicable standards 9
2. Purpose and Scope 9
2.1. Purpose 9
2.2. Scope 9
2.3. Netboss Comunicaciones' Objectives and Mission within the Framework of the Information Security Policy 10
2.4. Improvement Plan. Security Objectives 12
2.5. Legal Requirements 13
3. Organizational Context 13
3.1. Organizational Chart 13
3.2. IT Infrastructure 14
3.3. Stakeholders: Internal and External Relations 14
3.4. Stakeholder requirements and needs 17
4. Leadership 17
4.1. Management commitment 17
4.2. Information Security Policy Requirements 18
4.3. Information Security Policy 18
4.4. Roles, Responsibilities, and Authorities within the Organization 18
4.4.1. Safety Committee 18
4.4.2. Roles: Functions and Responsibilities 19
4.4.2.1. Management 19
4.4.2.2. Chief Information Officer 19
4.4.2.3. Head of Services 19
4.4.2.4. Security Manager 20
4.4.2.5. System Manager 20
4.4.2.6. Risk Owner 21
4.4.2.7. Asset Owner 21
4.4.2.8. Staff 22
4.4.3. Procedure for Designating Responsible Persons 22
4.4.4. Communication 22
4.5. Planning 23
4.5.1. Input Information for Planning 23
4.5.2. Planning Results. 24
5. Support 24
5.1. Resources 24
5.1.1. Resource provision 24
5.1.2. Infrastructure 24
5.2. People 25
5.3. Communication 25
5.4. Documented information 25
5.4.1. Control of Management System Documentation 25
5.4.2. System Documentation 26
6. Operation 28
6.1. Operational Planning and Control 28

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es

6.2. Information Security Risk Management 28
6.2.1. Risk Analysis Process 29
6.2.2. Risk Management Process 29
7. Monitoring 29
7.1. Process Monitoring and Measurement 29
7.2. Internal audit 30
7.3. Management Review 30
8. Continuous Improvement 30
8.1. Corrective and Preventive Action 31
9. Safety Principles 31
9.1. Asset Management 31
9.1.1. Liabilities associated with assets 31
9.1.2. Classification of information 31
9.2. Human Resources Management Security 32
9.3. Physical and Environmental Security 32
9.3.1. Secure Areas 32
9.3.2. Equipment Safety 33
9.4. Communications and Operations Management 33
9.4.1. Operating Procedures and Responsibilities 33
9.4.2. Management of Services Provided by Third Parties 34
9.4.3. Protection Against Malicious Code and Mobile Code 34
9.4.4. Backups 34
9.4.5. Network Security Management 35
9.4.6. Media Management 35
9.4.7. Information Sharing 36
9.4.8. Follow-up 36
9.5. Access Control 36
9.5.1. Business Requirements for Access Control 36
9.5.2. User Access Management 36
9.5.3. User Responsibilities 36
9.5.4. Network Access Control 37
9.6. Incident Management 37
9.7. Business continuity 37
9.8. Acceptable Use Policy 38

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es

5

RIGHTS OF USE:

GENDER CLAUSE:

All references in this Notice expressed in the masculine grammatical form, when referring to natural persons, shall be understood to refer equally to men and women and to their corresponding masculine or feminine adjectives.

REGULATORY UPDATE:

Netboss Comunicaciones S.L. reserves the right to update and modify these terms and conditions. The current terms and conditions can be viewed at https://app.factorialhr.com/my-documents/company-files/list

1. INTRODUCTION

1.1. About the Organization

Netboss Comunicaciones S.L. is one of Spain's leading consulting and outsourcing service companies.

We have three divisions that provide our clients with comprehensive solutions to their operational needs. Our consulting division, specializing in process reengineering and the design of information and customer/citizen service solutions; our BPO division, specializing in the outsourcing of front- and back-office services with our own contact center; and our Software Factory, our software division, with two proprietary products on the market: a powerful multi-sector scheduling, booking, and appointment platform; and a comprehensive field service management platform.

1.2. Importance of ICT Systems and Information Security

Netboss Comunicaciones S.L. relies on ICT (Information and Communications Technology) systems to achieve its objectives. These systems must be managed with due diligence, taking appropriate measures to protect them against accidental or deliberate damage that could affect the availability, integrity, confidentiality, authenticity, or traceability of the information processed or the services provided.

The goal of information security is to ensure the quality of information and the continuous provision of services by taking preventive measures, monitoring daily operations, and responding promptly to incidents.

ICT systems must be protected against rapidly evolving threats that have the potential to impact the availability, integrity, confidentiality, authenticity, traceability, intended use, and value of information and services. To defend against these threats, a strategy is required that adapts to changes in environmental conditions to ensure the continuous provision of services.

This means that the security measures required by the National Security Framework and data protection laws must be implemented, as well as continuously monitoring service levels, tracking and analyzing reported vulnerabilities, and preparing an effective incident response to ensure the continuity of services provided.

Netboss Comunicaciones S.L. must ensure that information security is an integral part of every stage of the system's lifecycle, from its conception through its decommissioning, including development or procurement decisions and operational activities. Security requirements and funding needs must be identified and included in planning, requests for proposals, and bid documents for ICT projects.

Netboss Comunicaciones S.L. must be prepared to prevent, detect, respond to, and recover from incidents, in accordance with the National Security Framework and data protection legislation.

This Security Policy follows the guidelines of CCN-STIC-805 from the National Cryptology Center, an agency attached to the National Intelligence Center.

1.3. General Concepts

The following security dimensions are addressed:

- Availability: the property or characteristic of assets whereby authorized entities or processes have access to them when required. It is necessary to ensure that system resources are available when needed, especially critical information.
- Integrity: the property or characteristic ensuring that information assets are not altered in an unauthorized manner. System information must be available exactly as it was stored by an authorized agent.
- Confidentiality: the property or characteristic ensuring that information is neither made available nor disclosed to unauthorized individuals, entities, or processes. Information must be available only to authorized agents, especially its owner.
- Authenticity: the property or characteristic ensuring that an entity is who it claims to be or that the source of the data is guaranteed. The system must be able to verify the identity of its users, and users must be able to verify the system's identity.
- Traceability: a property or characteristic whereby the actions of an entity can be attributed exclusively to that entity.

The PDCA cycle will be used throughout the entire lifecycle of the ISMS.

- P (Plan): In this phase, activities, responsibilities, and resources are established, along with the objectives to be achieved and how these objectives will be measured.
- D (Do): The processes are developed and implemented. Once implemented, the results of executing these processes must be measured.
- C (Check): The results are analyzed to verify whether the objectives have been achieved, and if not, to identify the causes.
- A (Act): The necessary actions are taken to correct any flaws detected in the processes or to improve them.

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es

1.4. Prevention

Netboss Comunicaciones S.L. must avoid, or at least prevent to the greatest extent possible, any compromise of information or services due to security incidents. To this end, the minimum security measures determined by the ENS and the GDPR will be implemented, as well as any additional controls identified through a threat and risk assessment.

These controls, along with the security roles and responsibilities of all staff, will be clearly defined and documented.

To ensure compliance with the policy, Netboss Comunicaciones S.L. must:

- Authorize the systems before they go live.
- Regularly a s s e s s security, including assessments of routine configuration changes.
- Request periodic third-party reviews to obtain an independent assessment.

1.5. Detection

Since services can rapidly degrade due to incidents—ranging from a simple slowdown to a complete outage—it is necessary to continuously monitor operations to detect anomalies in service delivery levels and act accordingly, as established in Article 9 of the ENS.

Monitoring is particularly relevant when establishing lines of defense in accordance with Article 8 of the ENS. Detection, analysis, and reporting mechanisms shall be established to notify those responsible, both on a regular basis and when a significant deviation from the parameters predefined as normal occurs.

1.6. Response

Netboss Comunicaciones S.L.:

- Establish mechanisms to respond effectively to security incidents.
- Designate a point of contact for communications regarding incidents detected in other departments or other organizations.
- Establish protocols for sharing information related to incidents involving customers and suppliers.

1.7. Recovery

To ensure the availability of critical services, Netboss Comunicaciones S.L. has developed ICT system contingency plans as part of its overall service continuity plan and recovery activities.

1.8. Applicable Standards

The standards that have served as a reference for the development of this Information Security Policy are as follows:

- UNE/ISO-IEC 27001 Standard: Information Technology. Specifications for Information Security Management Systems.
- Royal Decree 311/2022, of May 3, regulating the ENS. This is the primary framework establishing the basic principles and minimum requirements to ensure the adequate protection of information and electronic services.
- General Data Protection Regulation (GDPR) of May 25, 2018

2. Purpose and Scope

2.1. Purpose

The purpose of this document is to establish guidelines that ensure the security of information related to the services and products of Netboss Comunicaciones S.L. at an appropriate level based on the risk level of the assets and our needs and resources.

Information and the processes that support it are important assets for the company. The availability, integrity, and confidentiality of information are essential to maintaining the company's services, reputation, and image.

2.2. Scope

All guidelines described in this document shall apply to Netboss Comunicaciones S.L. as a whole, its facilities, and its assets:

- All departments, including both management and employees.
- Contractors, clients, or any other third party with access to Netboss Comunicaciones' information or systems.
- To databases, electronic and paper-based files, processing, equipment, media, programs, and systems.
- To information generated, processed, and stored—regardless of its medium or format—used in operational or administrative tasks.

- Information provided within an established legal framework, which shall be considered proprietary solely for the purpose of its protection.
- All systems used to administer and manage information, whether owned, leased, or licensed.

The scope of the Information Security Management System, in accordance with the National Security Framework, applies to the management of the following services and products:

- Corporate website.
- BPO and Contact Center.
- Consulting.
- Scheduling, appointment booking, and online reservation software.
- FSM (Field Service Management) software.

The scope of the Information Security Management System in accordance with the ISO/IEC 27001 standard applies to the management of the following services and products:

- Corporate website.
- BPO and Contact Center.
- Consulting.
- Scheduling, appointment booking, and online reservation software.
- FSM (Field Service Management) software.

Location

Netboss Comunicaciones S.L.

Plaza Vista Bahía, 1 – 2 Bajo, 39610 Astillero. Cantabria (Spain).

2.3. Objectives and Mission of Netboss Comunicaciones within the Framework of the Information Security Policy

Mission:
Our mission at Netboss Comunicaciones is to provide reliable, secure, and high-quality telecommunications solutions and digital services, ensuring the confidentiality, integrity, and availability of information. We are committed to complying with applicable legal, ethical, and regulatory standards, protecting the data of our customers, employees, and business partners, while fostering an environment of technological innovation and continuous improvement.

Objectives:

1. Protect the organization's information and assets:
   Ensure the security of our own and our customers' data against unauthorized access, loss, alteration, or misuse.
2. Comply with the applicable legal and regulatory framework:
   Implement and maintain security measures aligned with telecommunications industry laws and regulations, including international and national standards for information security.
3. Promote security awareness and accountability:
   Develop an organizational culture that promotes ongoing training and awareness of the importance of information security at all levels of the organization.
4. Ensure business continuity:
   Design and implement controls and risk management plans that ensure the uninterrupted operation of critical services, even in the event of security incidents or disasters.
5. Build trusting relationships with customers and partners:
   Protect the privacy of personal and business data, thereby strengthening Netboss Comunicaciones' credibility and reputation as a secure and reliable provider.
6. Adopt a strategy of continuous improvement:
   Periodically evaluate and update the security measures implemented, ensuring their effectiveness against emerging threats and regulatory changes.
7. Promote secure technological innovation:
   Integrate security practices from the design phase and throughout the entire lifecycle of the services and products offered by Netboss Comunicaciones.

These objectives reflect our commitment to excellence, security, and regulatory compliance, ensuring that every action and decision at Netboss Comunicaciones is aligned with our Information Security Policy.

Netboss Comunicaciones S.L. establishes this Security Policy, which is mandatory for all its employees, with the fundamental objective of ensuring information security and the continuous provision of the services it offers, by acting preventively, monitoring activities, and responding promptly to any incidents that may occur.

One of the objectives of this document is to establish guidelines that guarantee information security at Netboss Comunicaciones S.L. at an appropriate level, based on the risk level of the assets and the needs and resources of this organization.

This document must lay the groundwork to ensure that the access, use, custody, and safeguarding of the information assets used by Netboss Comunicaciones to carry out its functions are carried out under security guarantees in their various dimensions: Availability, Integrity, Confidentiality, Authenticity, and Traceability.

Based on these principles, the specific objectives of information security will be:

- To ensure information security in all its dimensions.

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es

- Formally managing security, based on risk analysis processes, to reduce or eliminate the risks inherent in our activities through the continuous improvement of security performance in our processes, products, and services.
- Develop, maintain, and test the contingency and business continuity plans defined for the various services offered.
- Properly manage incidents that affect information security (cyber incidents).
- Keep all staff informed about security requirements and promote best practices for the secure handling of information.
- Provide the security levels agreed upon with third parties when information assets are shared or transferred.
- Ensure that our current and future operations and processes comply with applicable information security legislation.

This Security Policy:

- Will be formally approved by the Management of Netboss Comunicaciones S.L...
- Will be reviewed annually to adapt to new technical or organizational circumstances and prevent obsolescence.
- Will be communicated to all employees.
- The Security Officer will be responsible for maintaining this policy and procedures and for providing support in their implementation.
- Each employee is responsible for complying with this policy and its procedures as they apply to their position.
- The heads of each department will be responsible for implementing this Policy and its corresponding procedures within their respective areas.
- This policy, as well as any future updates to it, will be made available to interested parties.

2.4. Improvement Plan. Safety Objectives

The Safety Committee will establish and approve an annual Improvement Plan that defines the safety objectives deemed necessary in each case to meet the stated goals. Objectives consistent with the defined safety policies must be established, and the necessary resources for their achievement must be provided, which will be defined in the Improvement Plan itself.

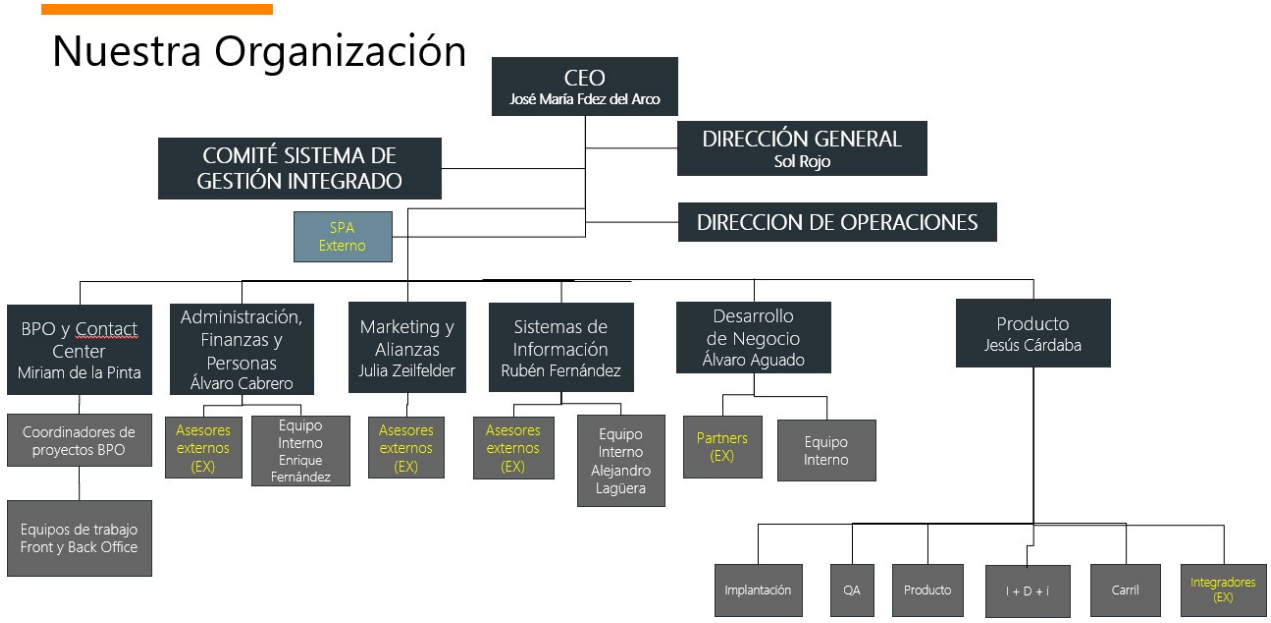
2.5. Legal Requirements

In order to fulfill the established commitments to comply with the laws and regulations applicable to the activities, products, and services of Netboss Comunicaciones S.L., the company has established and maintains the SGI P613 Legal Compliance procedure for the identification of and access to such legal requirements and other requirements to which the company is subject (agreements with public authorities, codes of good industrial practice, and non-regulatory guidelines or standards).
According to current legislation, the laws applicable to Netboss Comunicaciones S.L. for activities within the scope of the Management System are:

- Royal Decree 311/2022, of May 3, regulating the ENS. This is the primary framework establishing the basic principles and minimum requirements to ensure the adequate protection of electronic information and services.
- General Data Protection Regulation (GDPR) of May 25, 2018.
- Royal Legislative Decree 1/1996, of April 12, Intellectual Property Law.
- Industrial Property Law.
- Law 34/2002, of July 11, on Information Society Services and Electronic Commerce (LSSI).
- Cookie Directive
- European General Data Protection Regulation

3. ORGANIZATIONAL CONTEXT

3.1. Organizational Chart



3.2. IT Infrastructure

Netboss Comunicaciones S.L. has both servers and workstations. The servers are located in a dedicated room, which houses three cabinets: one for communications, one dedicated solely to servers, and another containing the telephone switchboard and two NAS devices for file storage. Cloud services are also outsourced to providers for various purposes, such as running virtual machines.

The workstations primarily run the Windows 11 Pro operating system. Regarding the server infrastructure, the VMware ESXi virtualization system, version 8.0, is used, with virtual servers running operating systems such as Windows Server 2025, Ubuntu Server, or Debian.

Internet access is provided via three fiber-optic lines. Internet access is filtered through a firewall to ensure the organization's security, and service continuity is also ensured through line load balancing.

An organizational network with an Active Directory manages user access permissions at workstations through user groups. Access control mechanisms are used to protect resources.
The information processed by the organization's employees is stored on dedicated file servers, with regular backups generated.

Technical infrastructure maintenance is performed by the company's specialized staff.

3.3. Stakeholders: Internal and External Relationships

The defined management system will take into account the various parties involved in the information system, primarily:

- Customers: As a fundamental part of the system, we will ensure the confidentiality, integrity, and availability of the information exchanged with customers and necessary for the provision of the services outlined in the scope, as well as any other information (administrative, contact, etc.) necessary for service delivery. Compliance with customers regarding data protection, specifically the GDPR.
- Suppliers: Given the importance of service providers for data processing, particularly regarding the IT services necessary for the provision of Netboss Comunicaciones S.L.'s services (such as software application providers or those responsible for IT maintenance tasks), the necessary requirements have been established to ensure the security and availability of their services. The transmission of information to financial institutions must also be taken into account.

- Public Administration: As recipients of the services provided by Netboss Comunicaciones S.L., in order to comply with applicable regulations and laws, the transmission of information will be carried out either through the means made available by such agencies for this purpose (web services) or through alternative means such as email (using an electronic signature) or magnetic media.
- Employees: As a key component in the processing of information, employees must be familiar with the security policies and procedures adopted by the organization to ensure the confidentiality, integrity, and availability of data.
- Competition: As a service provider to public administrations, Netboss Comunicaciones S.L. competes with other companies providing similar services in public tenders and for the award of minor contracts.
- Creditors and Financial Institutions: When financing is required, Netboss Comunicaciones S.L. applies for loans or other financial instruments from banks, other financial institutions, and/or companies or individuals offering financing.
- Shareholders/Company Owner: Currently, all shares of Netboss Comunicaciones S.L. are held by four shareholders.

The relationships between the various stakeholders included within the scope of the ISMS are detailed below:

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es

Service	Treatment system	Outsourced Services	Suppliers	Employees	Clients
Corporate website	Servers User equipment Applications Peripherals	Internet	Communications Providers	Development Department Systems Department	Public administrations Companies
Call Centers	Servers User Equipment Applications Peripheral equipment	Internet Telephone Network	Communications Providers	Call Center Department	Government Agencies Businesses
Consulting, Application Development and Implementation	Servers User Equipment Applications Auxiliary equipment	Internet	Communications Providers	Consulting Department Development Department Systems Department	Government Agencies Businesses
Cloud Services	Servers User Equipment Applications Peripheral equipment	Internet	Communications and Cloud Providers	Development Department Systems Department	Public Administrations Businesses

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es

3.4. Requirements and needs of stakeholders

Customers: Netboss Comunicaciones S.L. must comply with the contractual requirements established with customers for the provision of services.

Public Administration: Netboss Comunicaciones S.L. must comply with the legal or regulatory obligations established with the Public Administration.

Suppliers: Suppliers must comply with the terms set forth in the service level agreements regarding the security of the services provided, service and delivery deadlines, incidents, and the processing of personal data. For its part, Netboss Comunicaciones S.L. must comply with the contractual conditions as the service contractor and, in the event of processing suppliers' personal data, ensure the security of such data.

Employees: Employees must be familiar with and comply with the security policies, standards, and procedures applicable within the organization to ensure the confidentiality, integrity, and availability of data.

Creditors and Financial Institutions: Netboss Comunicaciones S.L. must comply with the financing terms established contractually with such entities, primarily by making loan repayment payments within the established timeframes.

Shareholders/Company Owners: Netboss Comunicaciones S.L. must comply with the objectives and strategic plans established by Management, aimed at achieving profitability for shareholders.

4. LEADERSHIP

4.1. Management Commitment

This Security Policy is a clear, explicit, and public policy of Netboss Comunicaciones S.L., and therefore management expresses its full support for it and commits to upholding the guidelines set forth in this Document. Likewise, it will publish and distribute the Policies and Regulations to all employees in the most appropriate manner, so that everyone is aware of the objective established by the Security Committee, the policies, principles, and standards adopted and their importance for the company's security, the general and specific security responsibilities of each member of the company, and other references to documentation that may be useful.

Management is committed to the implementation, maintenance, and improvement of the Management System, and therefore:

- It is committed to communicating to the organization the importance of meeting customer requirements, as well as legal and regulatory requirements.
- Establishes the Information Security Policy.

- Establishes the system's objectives and planning, as described in this Security Policy.
- Conducts reviews of the Management System
- Ensures the availability of resources.

4.2. Information Security Policy Requirements

It must be ensured that the Security Policy of Netboss Comunicaciones S.L.:

- Is appropriate for the organization's purpose and the nature of its activities, products, or services.
- It expressly includes a commitment to comply with applicable laws, regulations, and other requirements deemed appropriate.
- Provides a framework for establishing and reviewing the objectives of the Management System.
- It is communicated to and understood by the appropriate levels of the organization.
- It is reviewed to ensure ongoing suitability.
- The review will be conducted periodically, at least during the Management Review of the Management System (as established in this Security Policy), and on an ad hoc basis whenever Management deems it necessary.

The Security Policy will be made available to the public upon request, and Management ensures that this Policy is understood, implemented, and kept up to date within the organization.

4.3. Information Security Policy

The Information Security Policies are set forth in the "Security Principles" section.

4.4. Roles, Responsibilities, and Authorities within the Organization

4.4.1. Security Committee

The Security Committee coordinates information security at Netboss Comunicaciones S.L. and is composed of:

- Company Address.
- Data Controller.
- Head of Services.
- Security Officer.
- Systems Manager.

The Security Committee will meet at least once a year.

4.4.2. Roles: Functions and Responsibilities

To efficiently manage Information Security, each department at Netboss Comunicaciones S.L. must comply with the applicable policies and procedures. All such policies and procedures shall be approved by Management.

The members of the Security Committee are as follows:

- Head of Information Services: Company Management: CEO, General Manager, or their delegate. The CEO or General Manager is Jose María Fernández de Arco or Sol Rojo Vallejo
- Information Officer: Systems Director. Rubén Fernández Crespo
- Security Officer: Management System Officer. Sol Rojo Vallejo
- System Manager: Director of Systems, Rubén Fernández Crespo

The duties and responsibilities are detailed below:

4.4.2.1. Management

The Management of Netboss Comunicaciones S.L. is committed to fulfilling the obligations inherent to information security and protecting its information assets by implementing the most appropriate security measures to achieve this effectively with the available resources.

4.4.2.2. Information Officer The

Information Officer will be responsible for:

- The risk associated with all information.
- Ensuring the proper use of information and, therefore, its protection.
- Any error or negligence that leads to a breach of confidentiality or integrity.
- Establish information security requirements.
- Determine information security levels.

4.4.2.3. Head of Services Will be

responsible for:

- The risk associated with all Services.

- Establishing security requirements for the service, including requirements for interoperability, accessibility, and availability.
- Determining service security levels.

4.4.2.4. Security Officer

- This person is responsible for information security (including GDPR-related files).
- He is the Asset Owner for all company assets with regard to the ISO 27001 standard. In the asset inventory, an Asset Manager may be designated, to whom the Asset Owner delegates decision-making regarding that asset.
- He/she is responsible for the management and maintenance of the Management System.
- Ensures that the Management System processes are established, implemented, and maintained in accordance with the requirements of applicable standards.
- Reports to Management on the operation and effectiveness of the system so that Management can conduct a review, and as a basis for improving the company's management.
- Promotes awareness of customer requirements regarding Information Security at all levels of the organization.
- Collaborates with Management in defining and implementing Policies and Procedures so that they accurately reflect the company's strategy.
- Plans, schedules, and participates, as appropriate, in internal and external audits.
- Oversees the preparation, updating, approval, and distribution of Management System documentation.
- Acts as a liaison with external parties (customers, suppliers, government agencies, and other stakeholders) regarding aspects of the management system.
- Monitors the implementation and effectiveness of actions taken to prevent and manage nonconformities, and evaluates the actions to be taken following the submission of a suggestion for improvement.

4.4.2.5. System Manager Will be

responsible for:

- The risk of all assets, with the exception of essential assets (Services and Information).
- Developing, operating, and maintaining the Information System throughout its entire lifecycle, including its specifications, installation, and verification of proper operation.
- Defining the type and management system of the Information System by establishing the criteria for use and the services available within it.

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es

- Ensure that specific security measures are properly integrated into the overall security framework.
- The administration and management of user accounts.
- Ensure that only authorized individuals have access.
- Ensure that systems meet the availability levels required by the Organization.
- Include applicable security aspects in the requirements for new developments.

4.4.2.6. Risk Owner

The risk owner, associated with one or more information assets, shall have the following responsibilities:

- Participate in the development of the risk analysis and assessment conducted at least annually.
- Verify compliance with acceptable risk levels and collaborate in the approval of these (as they pertain to them), as well as the management of risks associated with information assets and the risks for which they are responsible.
- Ensure that staff immediately report any security breaches or misuse of information or systems to them. The risk owner must in turn inform the Security Officer to address the incident.
- Notify the Security Officer whenever there are changes in personnel, the organization, or other information assets that may require a review or update of the risk analysis or assigned access permissions.

4.4.2.7. Asset Owner

The asset owner, understood to be the person responsible for said asset, shall have the following responsibilities:

- Determine whether the asset is subject to the Data Protection Act and, if applicable, apply the corresponding procedures.
- Ensure that the software used is licensed.
- Determine who can access the information, how, and when, based on the classification of the information and the role to be performed.
- Ensure that the asset is properly maintained.

- Ensure that staff immediately report any security breaches or misuse of information or systems. The asset owner must in turn notify the Security Officer to address the incident.
- Ensure that staff have received adequate training, are familiar with and understand the Security Policy, and implement security guidelines.
- Ensure that media and equipment containing information are disposed of in accordance with established procedures.
- Implement the necessary security measures in your area to prevent fraud, theft, or service interruptions.
- Maintain up-to-date documentation of all critical functions to ensure business continuity in the event that someone is unavailable.
- Notify the Security Manager of any personnel changes that affect access to information or systems (change of role or department, leaving the company) so that access permissions can be updated accordingly.
- Where applicable, ensure that staff and contractors have confidentiality clauses in their contracts and are aware of their responsibilities.

4.4.2.8. Staff

- Know and understand the policies, regulations, and procedures that apply to your work.
- Ensure that your actions do not result in any security breaches.
- Report any actual or suspected security incident you detect to the asset owner.

4.4.3. Procedure for Designating Responsible Parties

The Security Officer will be appointed by Management upon the recommendation of the Security

Committee. The appointment will be reviewed every two years or whenever the position becomes vacant.

Management will also designate the System Manager, specifying their duties and responsibilities within the framework established by this Policy.

4.4.4. Communication

Netboss Comunicaciones S.L. ensures communication among the different levels and functions of the organization regarding the processes of the Management System and its effectiveness. Such communication consists of:

- Addressing and responding to staff concerns regarding the Management System.
- Communication among the organization's various operational areas to monitor the progress of the Management System's operational processes and to coordinate and standardize action criteria.
- Communication at the department level, in order to share among its members the knowledge and best practices acquired through experience during the development of the corresponding processes.
- Receiving, documenting, and responding to relevant communications from the organization's stakeholders, as well as ensuring internal communication among the various levels and functions of the organization.

To ensure such communication, the following procedures are followed:

- The Safety Manager, through regular departmental meetings with staff, internal email, etc., is responsible for communicating the Policies, objectives, goals, and progress of the Management System in general and the management of customer requirements in particular. These communications will take place whenever the Security Manager deems it appropriate and, in any case, following system reviews and audits, in order to disseminate the general and specific results and decisions arising from such activities.
- To ensure that specific urgent information is communicated to the affected staff, the organization has internal communication tools: email, Slack, Tiwsk, telephones, etc., which have a sender and one or more recipients, and which are used to communicate information regarding, for example, changes to an order that had already been conveyed to the affected personnel, the addition of a new person to the organization, the arrival of a visitor to the organization, etc.

A Communication Plan has been defined, detailing the communication channels between the various stakeholders, in document SGI D74 Communication Plan.

4.5. Planning

4.5.1. Input Information for Planning

Management Planning is carried out to establish the framework within which the company's improvement initiatives must be developed and guided.

The Management of Netboss Comunicaciones s.l., through the provisions of the established Management System, identifies and plans the necessary resources to:

- Achieve the Security Objectives.
- Ensure that organizational changes are implemented in a controlled manner and that the Management System maintains its integrity during these changes.

- Management Planning is carried out routinely during the System Review Meeting and on an ad hoc basis whenever Management so decides, and is documented in any case in the final minutes of such meetings.

4.5.2. Planning Outcome.

As a result of the planning, Management, in accordance with the defined Policies, establishes the organization's management objectives for each relevant level of the organization, which are included in the Improvement Plan and risk analysis report, containing:

- The approved objectives and targets.
- The assignment of responsibilities at each relevant function and level of the organization for the achievement of the objectives and targets.
- The resources and the timeline for when they must be achieved.

The objectives are measurable and are established (and reviewed) taking into account safety requirements, technological options, and financial, operational, and business requirements, as well as those necessary to meet the requirements for the product or service and the commitment to continuous improvement, customer feedback, and the views of stakeholders in general.

To assess the degree of compliance and ensure the adequacy and effectiveness of the system, the objectives are reviewed periodically, and the conclusions of their monitoring are discussed at Security Committee meetings, as detailed in the applicable procedure. The monitoring of the objectives is documented, recorded, and approved by the Committee.

5. SUPPORT

5.1. Resources

The purpose of this chapter is to describe how Netboss Comunicaciones S.L. manages its resources within the framework of its Management System.

5.1.1. Provision of Resources

Netboss Comunicaciones S.L. determines and provides, at the appropriate time, the resources necessary to implement and improve the Management System processes, and to achieve customer satisfaction, information security, and the delivery of services.

5.1.2. Infrastructure

Management is committed to the implementation, maintenance, and improvement of the Management System; therefore, it identifies, provides, and maintains the facilities necessary to achieve security objectives, including:

- Workspace and associated facilities.
- Equipment, hardware, and software.
- Support services.

The infrastructure necessary for the operations of Netboss Comunicaciones S.L. has been identified in the risk analysis.

5.2. People

Netboss Comunicaciones S.L. has established and maintains the SGI P71 Personnel Management procedure, which describes the criteria and associated responsibilities to ensure that personnel with defined responsibilities within the Management System are competent based on applicable education, training, awareness, practical skills, and experience.
Personnel security is essential for reducing the risks of human error, theft, fraud, or misuse of facilities and services.

5.3. Communication

A Communication Plan will be developed to establish the communication channels between the various stakeholders in the system (see document SGI D74 Communication Plan).

5.4. Documented Information

To implement this Management System, a document structure is in place consisting of:

- Security Policy, this policy: a document establishing the foundations of the company's Management System.
- Regulations: documentation defining permitted and prohibited uses within the organization.
- Procedures: describe the activities required to implement the Management System to comply with the requirements of applicable standards.
- Documents: any information in any format pertaining to the integrated management system.

The various documents are of an appropriate length to ensure the effective operation of the System and the organization, as well as the control of processes, depending on the complexity of the process, the interaction of the various processes, and the competence of the personnel involved.

5.4.1. Control of Management System Documentation

Netboss Comunicaciones S.L. has established and maintains an up-to-date ISMS management procedure that describes how the System's documentation should be controlled, including the criteria and responsibilities associated with controlling the documents necessary for the operation of the Management System.

5.4.2. System Documentation

ISO 27001	ENS	System Document
4. Organizational Context	org.1 Security Security	ISMS D51 01 Security Policy
4.1 Understanding the organization and its context		SGSI D51 01 Security Policy SGI P61 Risk Analysis and Management Risk Management
4.2 Understanding the needs and expectations of interested parties		ISMS D51 01 Security Policy
4.3 Determining the scope of the information security management system		ISMS D51 01 Security Policy ISMS D613 01 Scope Document
4.4 Information Security Management System		SGSI D51 01 Security Policy
5. Leadership		SGSI D51 01 Security Policy
5.1 Leadership and Commitment		SGSI D51 01 Security Policy SGI D3 Integrated Management System Manual
5.2 Policy	org.1 Security Security	SGSI D51 01 Security Policy
5.3 Roles, Responsibilities, and Authorities in the Organization	org.1 Security Security	SGSI D51 01 Security Policy
6. Planning		SGSI D613 01 Applicability Document SGS P843 Capacity Plan SGI P61 Risk Analysis and Management P61 Risk Analysis and Management SGI P71 Personnel Management
6.1 Actions to address risks and opportunities	op.pl.1 Risk analysis	SGI D10 03 Improvement Plan SGI P61 Risk Analysis and Management SGI P61-01 Risk Analysis and Management Report
6.2 Information Security Objectives and Planning for Their Achievement		SGI D10 03 Improvement Plan
7. Support		
7.1 Resources		SGSI D61 Risk Categorization SGI P61 Risk Analysis and Management SGI P61-01 Risk Analysis and Management Report SGI P84 01 Supplier Management
7.2 Competence	mp.per.4 Training	SGI P71 Personnel Management SGI D10 03 Improvement Plan

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es

ISO 27001	ENS	System Document
7.3 Awareness	mp.per.3 Awareness	SGI P71 Personnel Management SGI D10 03 Improvement Plan
7.4 Communication		SGSI D51 01 Security Policy SGI D74 Communication Plan
7.5 Documented Information		SGSI D51 01 Security Policy SGI D3 ISO Integrated Management System Manual SGI P71 Personnel Management
8. Operations		SGI D3 ISO Integrated Management System Manual
8.1 Planning and Operational Control		SGSI P858 Logical Security SGSI P854 Access Control SGSI P861 Incident Management SGSI P855 Physical Security SGI P75 02 Personal Data Protection SGI P75 01 Information Protection SGI P83 Software Development SGI P84 01 Vendor Management
8.2 Assessment of Information Security Risks	op.pl.1 Risk Analysis	SGI P61 Risk Analysis and Management SGI P61-01 Risk Analysis and Management Report P61 Risk Analysis and Management
8.3 Information Security Risk Treatment	op.pl.1 Risk Analysis	SGI P61 Risk Analysis and Management SGI P61-01 Risk Analysis and Management Report P61 Risk Analysis and Management
9. Performance Evaluation	op.mon.2 Metrics System	SGI D3 ISO Integrated Management System Manual
9.1 Monitoring, measurement, analysis, and evaluation	op.mon.2 Metrics System	SGI R91 Metrics and Indicators
9.2 Internal audit		SGI R92 01 audit program SGI R92 02 Internal audit report
9.3 Management Review		SGI R93 Management Review
10. Improvement		SGSI R10 Control NC – AC – OM – AM
10.1 Nonconformity and Corrective Actions		SGSI R10 control NC – AC – OM – AM
10.2 Continuous Improvement		SGSI R10 control nc – ac – om - am

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es

6. OPERATION

6.1. Operational Planning and Control

During service planning, the following points are determined as appropriate:

- Security objectives and service requirements.
- The need to establish processes and documents and to provide specific resources for the delivery of the service.
- The verification, validation, monitoring, and inspection activities specific to the product/service, as well as the criteria for its acceptance.
- The records necessary to provide evidence that the processes meet the requirements.

6.2. Management of Information Security Risks

Analyzing potential risks and developing a strategy to manage them appropriately is paramount for Netboss Comunicaciones S.L., since only by understanding the security status with rational evidence can the appropriate decisions be made to address any risks that arise.

Each asset is assessed in terms of Availability, Integrity, Confidentiality, Authenticity, and Traceability, using the criteria detailed in the SGSI D61 document on risk categorization.

The MAGERIT methodology ("Methodology for the Analysis and Management of Information System Risks") developed by the Higher Council for Electronic Administration was used to conduct the risk analysis.

The acceptable risk level will be documented in the SGI P61-01 Risk Analysis and Management Report.

MAGERIT covers risk analysis and treatment activities, facilitating informed risk management. The management of these risks will involve selecting and implementing the technical and organizational measures necessary to prevent, reduce, or control the identified risks, so that any harm they may cause is eliminated or, if this is not possible, reduced as much as possible.

Risk management is the comprehensive process of addressing the risks identified during the analysis.

6.2.1. *Risk Analysis Process*

- The assets of Netboss Comunicaciones S.L. will be identified. These assets are exposed to a series of threats that, when they occur, degrade the value of the asset, causing a certain impact.
- A series of threats that directly or indirectly affect the asset will be identified. By estimating the probability of the threat, we can determine the risk to the system or the loss to which it is exposed.
- The impact and probability determine the system's vulnerability to a threat.

6.2.2. *Risk Management Process*

Managing these risks will involve selecting and implementing the necessary technical and organizational measures to prevent, reduce, or control the identified risks, so that any harm they may cause is eliminated or, if this is not possible, reduced as much as possible.

You can choose from the following strategies to mitigate risk:

- Accept the risk: accept the risk and do not implement controls to reduce or eliminate it.
- Avoid the risk: eliminate the cause or consequence of the risk.
- Reduce the risk: limit the risk by implementing controls that reduce its impact.
- Transfer the risk: pass the risk on to others, such as an insurance company.

Safeguards will be implemented to address the threats.

Safeguards mitigate impact and risk levels, reducing them to residual values, which will be assumed by the Information Manager or the Service Manager.

The corresponding Applicability Document will specify for each ISO 27001 or ENS control whether it applies or not and the reason for that decision.

The risks and the controls adopted following the risk analysis must be reviewed annually, as well as whenever circumstances warrant. This shall be considered an integral part of security management.

7. MONITORING

7.1. Process Monitoring and Measurement

Process monitoring is carried out by checking a list of indicators approved by Management, which includes the frequency of monitoring, the person responsible for measurement, and the person responsible for data analysis.

If a deviation from the planned results is detected in the indicators, the Safety Manager must open a *"non-conformity"* to analyze the cause of the deviation and determine possible corrective actions.

7.2. Internal Audit

The purpose of this chapter is to describe the procedures and activities for planning and conducting internal audits of the Management System.

The Security Officer will review the policies annually or whenever significant changes warrant such a review, and will resubmit them to management for approval. The reviews will assess the effectiveness of the policies, evaluating the origin, number, and impact of incidents recorded since the implementation of the ISMS, the cost and impact of the established controls and the improvement measures adopted by the company, and the effects of technological changes. These reviews will include information systems, system providers, information owners and information asset owners, users, and Management.

The Management Committee of Netboss Comunicaciones S.L. will ultimately be responsible for approving the necessary modifications to the text whenever a change occurs that affects the assets originally assessed and the established risk situations.

The Information Security Management System will be audited according to an audit plan developed by the Security Officer. The ISMS will be fully audited every two years.

This point will be addressed in procedure SGI D3 of the Integrated Management System Manual.

7.3. Management Review

Management reviews its Information Security Management System to ensure its ongoing consistency, adequacy, and effectiveness. The review assesses the need for changes to the Management System, including the policy, objectives, and other elements, in light of the results of the system audit, changing circumstances, and the commitment to continuous improvement. All of this is documented in Procedure SGI D3: Integrated Management System Manual.

Based on the results of the review, a management plan is also established, which includes the objectives and goals for the next improvement cycle.

8. CONTINUOUS IMPROVEMENT

Netboss Comunicaciones S.L. is committed to the continuous improvement of the Management System. To this end, it relies on the Policies, objectives, results of internal audits, data analysis, corrective and preventive actions, and management review to facilitate continuous improvement.

8.1. Corrective and Preventive Action

In order to establish a process to reduce or eliminate the causes of nonconformity to prevent their recurrence, the SGI D3 Integrated Management System Manual procedure has been established and is kept up to date, defining the criteria and responsibilities associated with:

- the identification of actual or potential nonconformities
- determining the causes of nonconformity
- assessing the need to take action to ensure that nonconformities do not recur
- recording the results of the actions taken
- verification that the corrective or preventive action taken is effective.

9. Safety Principles

9.1. Asset Management

9.1.1. Responsibilities Related to Assets

To properly manage assets, the Security Manager will maintain an up-to-date inventory of important assets.

This inventory will record who owns the asset. This responsibility will be assigned to the person in charge of the area or department at Netboss Comunicaciones S.L. where the asset is physically or logically located.

9.1.2. Classification of Information

Information classification shall be in accordance with the following scale:

Confidential	Information that should only be accessible to certain individuals or departments within the organization. If it were leaked to third parties, it could have serious consequences for the organization
Internal Use	Information that should only be accessible to the organization's staff. If leaked to third parties, it could have consequences for the organization.
Public	Information for which there is no need to restrict access. If leaked to third parties, it would have no consequences for the organization.

A list of information at Netboss Comunicaciones S.L. will be maintained with its corresponding classification (Confidential/Internal Use/Public). Netboss Comunicaciones S.L. staff will be made aware of this classification so that they know at all times the type of information they are using, without the need to mark it, thereby not revealing the classification to external sources

information. The destruction of this information shall be carried out by the person responsible for the asset, in accordance with the guidelines approved by the Security Officer and with the Security Officer's assistance if necessary.

9.2. Human Resources Management Security

Security related to personnel is essential to reduce the risks of human error, theft, fraud, or misuse of facilities and services.

The hiring of personnel involves a selection process in which references and background checks must be conducted whenever possible.

The terms of the employment relationship must clearly outline the employee's responsibilities regarding information security. This responsibility will continue for a specified period after the contract ends.

All employees must sign a confidentiality agreement to prevent the disclosure of confidential information.

All safety policies and procedures must be communicated regularly to all employees and third-party users, as appropriate. Seminars will be held periodically to ensure that staff are familiar with the safety procedures and tasks they are required to perform.

Employees who violate safety regulations may be subject to disciplinary action in accordance with the general agreement.

Upon termination of the employment or contractual relationship with employees or external personnel, their access permits to the facilities and information will be revoked, and they will be required to return any information or equipment provided to them for the performance of their duties.

9.3. Physical and Environmental Security

For logical security to be effective, it is essential that the facilities of Netboss Comunicaciones S.L. must maintain adequate physical security to prevent unauthorized access, as well as any other type of damage or external interference.

9.3.1. Secure Areas

- Netboss Comunicaciones S.L. will take the necessary precautions to ensure that only authorized persons have access to the facilities.
- All Netboss Comunicaciones S.L. offices are equipped with the necessary physical barriers to secure the resources they house.
- The areas where the server and cabling are located will be locked, and access will be restricted to authorized personnel and service providers only when accompanied by an authorized individual.
- Windows and doors must remain closed when the facilities are unoccupied.

- The facilities of Netboss Comunicaciones S.L. are equipped with fire extinguishing devices in accordance with current legislation on the matter. In this regard, fire extinguishers and emergency exits are available and properly marked.
- Staff are expressly prohibited from eating or drinking near servers and computer equipment. Likewise, special care must be taken when handling any product that could spill onto information assets.
- To prevent water leaks and flooding, periodic inspections of faucets, toilets, and other fixtures that could cause such damage are required.

9.3.2. Equipment Security

- Computer equipment is a critical asset upon which the continuity of the organization's operations depends; therefore, it must be adequately and effectively protected.
- Both user workstations and servers are protected against potential power outages or other electrical anomalies; to this end, uninterruptible power supply (UPS) systems have been installed.
- Equipment must be properly maintained to ensure its correct operation and optimal condition, thereby safeguarding the confidentiality, integrity, and, above all, availability of the information. To this end, they must undergo the inspections recommended by the supplier. Only duly authorized personnel may access the equipment to perform repairs. It will also be necessary to take the necessary precautions if the equipment must be removed from the premises for maintenance.
- Equipment disposal shall only be carried out by the Security Officer or personnel to whom the Security Officer delegates this responsibility.

9.4. Communications and Operations Management

9.4.1. Operating Procedures and Responsibilities

Netboss Comunicaciones S.L. will control access to services on internal and external networks and ensure that users do not compromise those services. To this end, it must establish appropriate interfaces between the Netboss Comunicaciones S.L. network and other networks, as well as appropriate authentication mechanisms for users, devices, and access rights for each user of the information system.

To prevent malicious use of the Netboss Comunicaciones S.L. network, mechanisms will be in place to govern the network services that can be accessed, authorization procedures to determine who can access which network resources, and management controls to protect network access.

All employees authorized to handle automated information must be registered as users of the information system. Each time they access the information system, they must authenticate themselves using their username—which is unique and non-transferable—and their personal password.

To ensure the correct and secure operation of information systems, operating procedures shall be properly documented and implemented in accordance with these procedures. These procedures shall be reviewed and appropriately modified when significant changes in equipment or software so require.

9.4.2. Management of Services Provided by Third Parties

When Netboss Comunicaciones S.L. contracts an external service to manage information assets, it introduces new vulnerabilities into the process, as resources are exposed to potential damage, loss, or data breaches. For this reason, it will be necessary to take a series of precautions to ensure the proper use of Netboss Comunicaciones S.L.'s information.

Before contracting an external service for information management, Netboss Comunicaciones S.L. will identify the risks involved in this situation and draft an agreement addressing the following issues: which applications are retained at Netboss Comunicaciones S.L. due to their critical nature, the approval of the application owners, the implications of the contract for business continuity plans, security standards and how their effectiveness will be measured, who is responsible and what special procedures will be followed to monitor important security activities, who will handle security incidents and how, and through what procedures Netboss Comunicaciones S.L. will be informed of such incidents.

9.4.3. Protection against Malicious Code and Mobile Code

The installation of any software other than that permitted and necessary for the performance of work by Netboss Comunicaciones S.L. staff is strictly prohibited.

All software acquired by the organization, whether through purchase, donation, or transfer, is the property of the institution and retains the rights conferred by intellectual property law, with due attention to the various types of licenses.

Any software that needs to be installed to work on the network must be evaluated by management.

The Security Officer will oversee the installation of appropriate IT tools to protect systems against viruses, worms, Trojans, etc., and users must follow the guidelines provided to protect the equipment, applications, and information they work with.

9.4.4. Backups

Data must be stored in a network directory to ensure that backups are performed regularly.

Procedures will be established for creating backups, which will be archived to enable data recovery in the event of an incident. These backups will be clearly labeled and stored in a secure location, preferably off-site.

Procedures will also be developed to recover data from the backups. It is necessary to periodically verify that the information is stored correctly and allows for the restoration of a minimum level of service if necessary.

If operational data becomes corrupted, the relevant software, hardware, and communications must be checked before using the backups to ensure that the data contained in them cannot also be corrupted.

9.4.5. Network Security Management

All computer equipment (workstations, servers, etc.) that is connected to the network, or those that are standalone and owned by Netboss Comunicaciones S.L., must comply with the installation standards and procedures issued by the IT department and previously approved by management.

Network equipment (switches, routers, etc.) will be kept out of reach of unauthorized personnel to prevent malicious use that could compromise system security.

9.4.6. Media Management

Users shall apply the same security measures to media containing sensitive information as to the files from which they were extracted.

Media (both paper and digital) containing sensitive information must be kept in locked drawers or cabinets. When an authorized person needs to use such media to perform tasks related to company business, they will be responsible for taking proper care of the media. They must not leave them on their desk when leaving their workstation, nor place them in any other location where an unauthorized person could see or take them.

Reusable media that no longer contain necessary information must be erased, provided the appropriate authorization has been obtained. This disposal must be carried out securely to prevent the data it contains from being leaked to others. Some destruction methods considered appropriate include incineration, shredding, or erasing the media so that they can be reused for another application within Netboss Comunicaciones S.L.

It is always necessary to document the disposal of media containing sensitive information to maintain an audit trail.

9.4.7. *Information Exchange*

Procedures will be established to protect information exchanged through any means of communication (electronic, verbal, fax, etc.).

9.4.8. *Monitoring*

As deemed necessary, the necessary mechanisms will be established to detect unauthorized information processing activities. This will involve performing tasks to carry out controls and inspections of system logs and activities to test the effectiveness of data security and data integrity procedures, to ensure compliance with the established policy and operating procedures, as well as to recommend any changes deemed necessary.

9.5. Access Control

9.5.1. *Business Requirements for Access Control*

Information must be protected against unauthorized access.

Each department or area manager will define information access requirements at two levels: for the department or area as a whole, and for each user within that group. Access will only be granted to the information necessary for the work to be performed.
In the event that visitors or unauthorized personnel access the facilities or information of Netboss Comunicaciones S.L., they must always be accompanied by a responsible member of Netboss Comunicaciones S.L., who will ensure at all times that the security of the resources is maintained.

9.5.2. *User Access Management*

The IT Manager is responsible for providing users with access to IT resources, as well as specialized logical access to resources (servers, routers, databases, etc.) connected to the network.

Each user must be assigned a profile, based on the tasks they perform within the organization, as defined by their direct supervisor. Each of these profiles will have specific permissions, and access to information and systems not necessary for their job duties will be restricted.

9.5.3. *User Responsibilities*

Staff workstations must be kept clear of papers and other information storage media to reduce the risk of unauthorized access, as well as other potential damage. These should be stored in appropriate locked spaces, especially outside of working hours.

Similarly, computer equipment must be configured to lock when the user is away from their workstation, requiring a password to access the data stored on the device.

Mail inboxes and outboxes, fax machines, and printers that are not supervised by a Netboss Comunicaciones S.L. employee must also be protected.

9.5.4. Network Access Control

No user who is not formally authorized to do so will be permitted access to the network, systems, applications, or information.

In the case of service providers or external entities that need to access them for a justified reason, they are required to sign confidentiality agreements with the organization to maintain the same level of security as if they were employees of Netboss Comunicaciones S.L.

The Security Officer will manage the registration and deactivation of all users.

9.6. Incident Management

Any employee who suspects or observes a security incident—whether physical (fire, water, etc.), software or systems-related (viruses, data loss, etc.), or involving support services (communications, electricity, etc.)—must immediately report it to the Security Officer so that appropriate measures can be taken and the incident recorded.

Responsibilities and incident management procedures will be established to ensure a rapid, effective, and orderly response to security-related events.

The incident log will serve as a basis for identifying new risks and for verifying the effectiveness of the controls in place.

9.7. Business Continuity

It is essential for Netboss Comunicaciones S.L. to establish guidelines for action to be taken in the event of a disruption to business activities due to serious security breaches or disasters of any kind.

To ensure business continuity in such cases, Netboss Comunicaciones S.L. will establish contingency plans that allow for the resumption of operations at least to a minimum level within a reasonable timeframe. Business continuity management will therefore include various controls for identifying and mitigating risks, as well as a procedure to limit their harmful consequences and ensure the resumption of essential operations as quickly as possible.

The business continuity strategy will be documented, based on the identified risks and the controls defined accordingly, which must be tested and updated regularly to verify their suitability.

Business continuity management will be incorporated into the processes of Netboss Comunicaciones S.L. and will be the responsibility of one or more individuals within the company.

9.8. Acceptable Use Policy

Information systems and information shall be used solely for the purposes for which they have been made available to users. The following is not considered acceptable:

- The creation or transmission of material that violates data protection or intellectual property laws.
- Installing, modifying, or changing the configuration of software systems (only system administrators are authorized to do so).
- The use of assets for personal purposes is not permitted. Any personal electronic transactions carried out are the sole responsibility of the user.
- Deliberately providing access to facilities or services to unauthorized persons.
- Deliberately wasting network resources or system resources.
- Intentionally corrupting or destroying other users' data or violating their privacy.
- Deliberately introducing viruses or other forms of malicious software. Before using any data storage medium, you must verify that it is free of viruses or similar threats.
- Voluntarily disclosing passwords and means of access.
- Using the equipment for personal gain.
- The creation, use, or transmission of material that is offensive, obscene, or likely to cause distress or offense.
- Sending very large email messages or to a very large group of people (which could overload the system).
- Failing to verify that emails are free of viruses.

Likewise, users must take the following security measures into account when processing information and using IT systems:

- Anyone who suspects or observes a security incident—whether physical (fire, water, etc.), software or systems-related (viruses, data loss, etc.), or involving support services (communications, electricity, etc.)—must immediately report it to the Security Officer so that appropriate measures can be taken and the incident recorded.
- Each user's computer workstation shall be under the responsibility of an authorized user, who shall endeavor, to the best of their ability, to protect the confidentiality of company information—and, in particular, the personal data to which they have access—against unauthorized disclosure or any other form of manipulation or misuse.

- When the person responsible for a computer temporarily leaves it, they must leave it in a state that prevents the viewing of protected data, by locking the user account and preventing use of the workstation. Resuming work will require deactivating the screen saver by entering the corresponding password. If the computer is left due to the end of a work shift, the user must restart or shut down the system.
- All documents containing company information must be removed from printers and other output devices as they are printed.
- No user may use removable devices (CDs, DVDs, USB drives, etc.) or store information on them without prior authorization from the Security Officer.
- Media containing information must be clearly identified with an external label indicating (directly or indirectly) which file it is and what type of data it contains.
- Media containing information must be stored in a secure, locked location, or in rooms, offices, etc., with restricted access, when not in use, especially outside of working hours.
- No user may install or run programs that could interfere with the work of other users or damage or alter any of the computer resources. Under no circumstances may users install illegal or unauthorized copies of programs, nor may they delete any legally installed programs.
- It is strictly prohibited to modify the configuration of any software—whether operating systems or applications—set by default on the computer by the Security Officer without their prior authorization.
- The use of email and the Internet must be limited to work-related functions.
- Do not reply to fake emails or chain letters to prevent your email address from being shared. Do not open suspicious attachments from unknown senders or those that were not requested.
- If viruses are detected in received files or emails or while browsing the Internet, the Security Officer and the IT department must be notified.
- Passwords will be assigned to all system users as a means of verifying their identity. The password assignment procedure is carried out through personal delivery by the IT Manager, who is responsible for providing the username and password for system access. For some platforms, two-factor authentication will be required.
- The password must consist of at least 14 characters (it must include at least 3 of the following 4 characteristics: uppercase letters, lowercase letters, numbers, or special characters) and must not be disclosed under any circumstances, nor should it be kept in writing or in plain view of third parties.
- It is recommended to change passwords every two months. Additionally, devices must have screen savers that activate after ten minutes of inactivity, requiring a password to unlock the screen.
- The password must not contain the account ID or username, or any

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es

other personal information that is easy to guess (birthdays, children's names, spouses' names, etc.). Nor should you use a sequence of letters that are next to each other on the keyboard (123456, QWERTY, etc.).

- It is not recommended to use the same password for all accounts created to access online services. If any of them is compromised, all other accounts protected by that same password should also be considered at risk.
- Do not share passwords online, via email, or over the phone. In particular, be wary of any email message asking for your password or instructing you to visit a website to verify it.
- If a user has reasonable grounds to suspect that their authorized access is being or may be used by another person, they are required to change their password and must contact the Security or IT Manager to report the incident.
- No one may use another user's authorized access, even if authorized by the account holder.
- No user shall attempt to access restricted areas of their own or third-party information systems other than those assigned to them.

Laptops and mobile phones will be assigned by Netboss Comunicaciones S.L. There will be an up-to-date inventory of laptops and mobile phones. Netboss Comunicaciones S.L. will be responsible for managing this inventory.

- These devices shall be in the custody of the user or the designated representative of Netboss Comunicaciones S.L. Both parties must take the necessary measures to prevent damage or theft, as well as unauthorized access. The theft of this equipment must be immediately reported to Netboss Comunicaciones S.L. so that appropriate measures can be taken and the item removed from the inventory.
- Laptops and mobile devices must be used solely for business purposes, especially when used outside the premises of Netboss Comunicaciones S.L.
- Users of this equipment are responsible for ensuring that it is not used by third parties outside of Netboss Comunicaciones S.L. or by unauthorized individuals.
- Mobile devices will require user authentication to access them, as well as the installed applications.
- In general, portable devices must not be connected directly to external networks (including the user's home network or Internet access). In duly justified cases and with prior authorization from Netboss Comunicaciones S.L., alternative connections may be used, provided strict security measures are observed regarding Internet browsing and all other applicable provisions of these General Regulations.
- Connections to open Wi-Fi networks, such as those provided in airports, hospitals, shopping centers, etc., are prohibited, as these networks are not secure and information may be extracted from communications established during the connection.
- Additional software must be used to protect devices through the use of

antivirus systems, as well as actions such as remote tracking and wiping in the event of loss.

Plaza Vista Bahía, 1-2. 39610 El Astillero. Cantabria (Spain)
+34 942010701 info@netboss.es
www.netboss.es