netboss®
COMUNICACIONES

Successful projects made with
talent, technology and passion.

SGSI D51 01 Information Segurity Policy

Santander (ES), September 8, 2022
Versión: 1.7

Version control

Version control			
Date	Author	Version	Changes
29.12.2017	Management systems management	1.0	Initial version
08.02.2019	Management systems management	1.1	Updating points 1.8, 2.5, 3.2 and 3.3
05.07.2019	Management systems management	1.2	Updating item 3.1
16.09.2019	Management systems management	1.3	Format update
23.07.2020	Management systems management	1.4	Updating point 3.1 and organization chart
04.03.2021	Management systems management	1.5	Organization chart update
22.02.2022	Management systems management	1.6	Updating and revision
08.09.2022	Administration Department	1.7	Updating item 3.1
27/02/2024	Management systems management	1.8	Updating of organization chart and item 9.8
Document reviewed and approved by management - Valid without signature			

CONTENT

RIGHTS OF USE:

The present documentation is property of Netboss Comunicaciones S.L., and is confidential. It may not be reproduced in whole or in part, processed by computer or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise.

GENDER CLAUSE:

All references contained in this Communiqué expressed in the grammatical masculine, when referring to natural persons, should be understood to refer indistinctly to men and women and to their corresponding masculine or feminine adjectivations.

REGULATORY UPDATE:

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

1. Introduction

1.1. Presentation of the Organization

Netboss Comunicaciones S.L. is one of the leading Spanish consulting and outsourcing services companies. We have three divisions that provide our clients with an integral solution to their operational needs. Our consulting division, specialized in process reengineering and the design of information and customer/citizen services; our BPO division, specialized in the outsourcing of front and back office services with its own contact center; and our Software Factory, our software division, with two proprietary products in the market: a powerful multi-sector scheduling, booking and appointment scheduling platform; and a complete field service management platform.

1.2. Importance of ICT systems and information security

Netboss Comunicaciones S.L. depends on ICT (Information and Communication Technologies) systems to achieve its objectives. These systems must be managed diligently, taking appropriate measures to protect them against accidental or deliberate damage that may affect the availability, integrity, confidentiality, authenticity, or traceability of the information processed or services provided.

The objective of information security is to guarantee the quality of information and the continuous provision of services, acting preventively, monitoring daily activity and reacting promptly to incidents.

ICT systems must be protected against rapidly evolving threats with 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 that adapts to changing environmental conditions is required to ensure continuous service delivery.

This implies implementing the security measures required by the National Security Scheme and the data protection legislation , as well as continuously monitoring service delivery levels, tracking and analyzing reported vulnerabilities, and preparing an effective response to incidents to ensure the continuity of the services provided.

Netboss Comunicaciones S.L. must ensure that information security is an integral part of every stage of the system's life cycle, from its conception to its decommissioning, through development or acquisition decisions and operational activities. Security requirements and funding needs should be identified and included in planning, request for bids, and bidding documents for ICT projects.

Netboss Comunicaciones S.L. must be prepared to prevent, detect, react and recover from incidents, according to the National Security Scheme and data protection legislation.

This Security Policy follows the indications of the guide CCN-STIC-805 of the National Cryptologic Center, a center attached to the National Intelligence Center.

1.3. General Concepts

The following safety dimensions are contemplated:

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

The PDCA cycle is the one that will be used during the entire life cycle of the ISMS.

- **P (Plan):** in this phase the activities, responsibilities and resources are established, as well as the objectives to be met and how these objectives will be measured.
- **D (Develop):** processes are developed and implemented. Once implemented, the results of the execution of 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 the failures detected in the processes or to improve them.

1.4. Prevention

Netboss Comunicaciones S.L. must avoid, or at least prevent as far as possible, that the information or services are harmed by security incidents. For this purpose, the minimum security measures determined by the ENS and the RGPD will be implemented, as well as any additional control identified through a threat and risk assessment.

These controls and the security roles and responsibilities of all personnel will be clearly defined and documented.

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

- Authorize systems before going into operation.
- Regularly evaluate security, including evaluations of configuration changes made on a routine basis.
- Request periodic review by third parties in order to obtain an independent assessment.

1.5. Detection

Given that services can degrade rapidly due to incidents, ranging from simple slowdowns to stoppage, it is necessary to monitor the operation continuously to detect anomalies in service delivery levels and act accordingly as established in Article 9 of the ENS.

Monitoring is especially relevant when establishing lines of defense in accordance with Article 8 of the ENS. Detection, analysis and reporting mechanisms shall be established to reach those responsible, both on a regular basis and when there is a significant deviation from the parameters that have been pre-established as normal.

1.6. Reply

Netboss Communications S.L.:

- Establishes mechanisms to respond effectively to security incidents.
- Designates a point of contact for communications regarding incidents detected in other departments or other agencies.
- Establishes protocols for the exchange of information related to incidents with customers and suppliers.

1.7. Recovery

To guarantee the availability of critical services, Netboss Comunicaciones S.L. has developed contingency plans for ICT systems as part of its general service continuity plan and recovery activities.

1.8. Applicable standards

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

- **Standard UNE/ISO-IEC 27001 Information Technology.** Specifications for Information Security Management Systems.
- **Royal Decree 3/2010**, of January 8, **2010**, which regulates the **National Security Scheme** (ENS) in the field of Electronic Administration, article 11 of which establishes the obligation for Public Administrations to have a Security Policy and indicates the minimum requirements to be met.
- **Royal Decree 951/2015**, of October 23, amending Royal Decree 3/2010, of January 8, which regulates the National Security Scheme in the field of Electronic Administration.
- **General Data Protection Regulation (GDPR)** of 25/05/2018.

2. Purpose and field of application

2.1. Object

This document aims to establish guidelines to ensure the security of the information of the services and products of Netboss Comunicaciones S.L. at an appropriate level according to the level of risk 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 maintain the services and the reputation and image of the company.

2.2. Scope

All guidelines described herein shall be effective for Netboss Comunicaciones S.L. as a whole, its facilities and assets:

- To all departments, both managers and employees.
- To contractors, customers or any other third parties who have access to Netboss Communications information or systems.
- To databases, electronic and paper files, processing, equipment, media, programs and systems.
- Information generated, processed and stored, regardless of its support and format, used in operational or administrative tasks.
- To the information transferred within an established legal framework, which will be considered as its

own for the sole 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 Scheme applies to the management of the following services and products:

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

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

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

Location

Netboss Communications S.L.
Plaza Vista Bahía, 1 - 2 Bajo, 39610 Astillero. Cantabria (Spain).

2.3. Management System Objectives

Netboss Comunicaciones S.L. defines the present Security Policy , of obligatory character for all its employees, having as fundamental objective to guarantee the security of the information and the continued provision of the services that it provides, acting preventively, supervising the activity and reacting promptly in front of the incidents that can occur.

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

This document must lay the foundations so that the access, use, custody and safeguarding of the information assets, which Netboss Communications uses to develop its functions, are carried out under security guarantees, in its different dimensions: Availability, Integrity, Confidentiality, Authenticity and Traceability.

Under these premises, the specific objectives of Information Security will be:

- Ensure the security of information, in its different dimensions.
- Formally manage safety, based on risk analysis processes, to reduce or eliminate the risks inherent to our activities through continuous improvement of safety performance in our processes, products and services.
- Develop, maintain and test the contingency and business continuity plans defined for the different services offered.
- Perform an adequate management of incidents affecting information security (cyber incidents).
- Keep all personnel informed about security requirements, and disseminate good practices for the secure handling of information.
- Provide the security levels agreed with third parties when sharing or transferring information assets.
- To ensure that our current and future operations and processes comply with current legislation on information security.

This Security Policy:

- It will be formally approved by the Management of Netboss Comunicaciones S.L....
- It will be reviewed annually, so as to adapt to new technical or organizational circumstances and avoid obsolescence.
- It will be communicated to all employees.
- The Security Manager will be responsible for maintaining this policy , the procedures and for providing support in its implementation.
- Each employee is responsible for complying with this policy and its procedures as applicable to his or her job.
- The heads of each department shall be responsible for implementing this Policy and its corresponding procedures within their area.
- This policy, as well as future developments of this policy, will be made available to interested parties.

2.4. Improvement Plan. Security Objectives

The Security Committee will establish and approve an annual Improvement Plan, which will define the security objectives considered necessary in each case to comply with the indicated objectives. Objectives consistent with the defined security policies must be established, and the necessary resources must be provided for their achievement, which will be defined in the Improvement Plan itself.

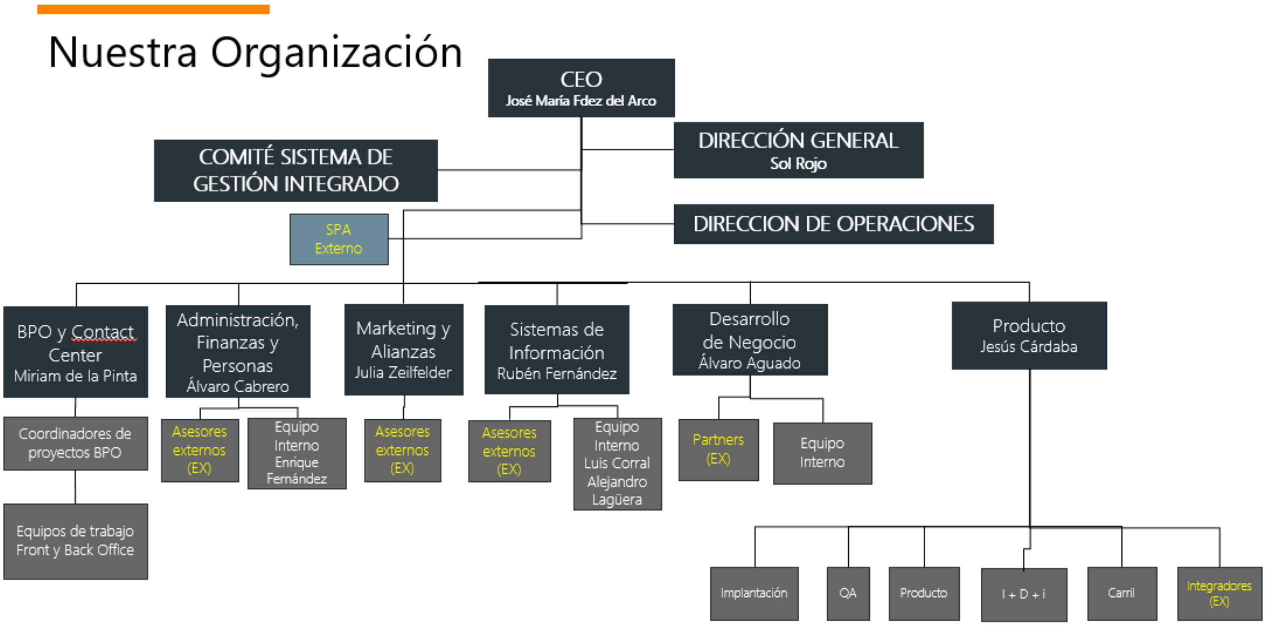
2.5. Legal Requirements

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

- **Royal Decree 3/2010**, of January 8, **2010**, which regulates the **National Security Scheme** (ENS) in the field of Electronic Administration, article 11 of which establishes the obligation for Public Administrations to have a Security Policy and indicates the minimum requirements to be met.
- **Royal Decree 951/2015**, of October 23, amending Royal Decree 3/2010, of January 8, which regulates the National Security Scheme in the field of Electronic Administration.
- **General Data Protection Regulation (GDPR)** of 25/05/2018.
- Royal Legislative Decree 1/1996, of April 12, 1996, **Intellectual Property Law**.
- Industrial Property Law.
- Law 34/2002, of July 11, 2002, on **information society services** and electronic commerce (LSSI).
- Cookies Directive
- European Data Protection Regulation

3. CONTEXT OF THE ORGANIZATION

3.1. Organization chart



3.2. IT infrastructure

Netboss Comunicaciones S.L. has both servers and workstations. The servers are located in a specific room, where there are three cabinets, one for communications, one dedicated only to servers and another with the PBX and two NAS file storage. Cloud services are also outsourced to providers with different uses, such as the execution of virtual machines.

Windows Operating System is mainly used in the workstations, in its Windows 11 Pro version. Regarding the server structure, the virtualization system VMware Esxi version 8.0 is used, with virtual servers with both Windows Server 2022 and GNU/Linux operating systems, mainly Ubuntu Server 22.04.

Internet access is available through three fiber optic lines. Internet access is filtered by means of a firewall to guarantee the security of the organization. The continuity of the service is also guaranteed by means of line balancing and a cluster with two passive active firewalls.

There is an organizational network with an Active Directory that manages user access permissions on workstations by means of user groups. Access control mechanisms are used to protect resources.
The information processed by the entity's employees is stored in file servers designed for this purpose, generating periodic backup copies of the same.

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

3.3. Stakeholders: Internal and external relations

The management system defined will take into account the different parties involved in the information system, mainly:

- Customers: as a fundamental part of the system, care will be taken to preserve the confidentiality, integrity and availability of the information exchanged with customers, and necessary for the provision of the services indicated in the scope, as well as any other information (administrative, contact…) necessary for the provision of the service. Adequacy with customers in terms of Data Protection, specifically to the RGPD regulation.
- Suppliers: Due to the relevance of service providers for the processing of information, especially in terms of IT services necessary for the provision of Netboss Comunicaciones S.L. services (such as suppliers of computer applications, or those responsible for computer maintenance tasks), the necessary requirements have been established to ensure the security and availability of their services. The information sent to the banking entities must also be taken into account.
- Public Administration: As recipients of the services provided by Netboss Comunicaciones S.L., in order to comply with the rules and laws of application, the sending of information will be done either through the means that these agencies make available for this purpose (web services) or by alternative means such as email (by electronic signature) or magnetic media.
- Employees: As a fundamental part of information processing, employees must be familiar with the security standards and procedures that the organization decides to apply to ensure the confidentiality, integrity and availability of data.
- Competition: As a provider of services to public administrations, Netboss Comunicaciones S.L. competes with other companies, providers of similar services, in public tenders, and for obtaining minor contracts.
- Creditors and Financial Entities: When financing is required, Netboss Comunicaciones S.L. requests loans, or other financial instruments, from banks, other financing entities and/or companies/individuals that offer financing.
- Shareholding/Ownership of the company: Currently all the shares of Netboss Comunicaciones S.L. are held by four shareholders.

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

Service	Treatment system	Outsourced services	Suppliers	Workers	Customers
Corporate website	Servers Job openings Applications Auxiliary equipment	Internet	Communications Providers	Development Department Systems Department	Public Administrations Companies
Call Center	Servers Job openings Applications Auxiliary equipment	Internet Telephone Network	Communications Providers	Call Center Department	Public Administrations Companies
Consulting, Development and implementation of applications	Servers Job openings Applications Auxiliary equipment	Internet	Communications Providers	Consulting Department Development Department Systems Department	Public Administrations Companies
Cloud Services	Servers Job openings Applications Auxiliary equipment	Internet	Communications and Cloud Providers	Development Department Systems Department	Public Administrations Companies

3.4. Stakeholder requirements and needs

Clients: 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: The suppliers must comply with the conditions established in the service level agreements formalized regarding the security of the services provided, the terms of provision and delivery, the incidences and the treatment of personal data. Netboss Comunicaciones S.L. shall comply with the contractual conditions as service contractor and in case of processing personal data of suppliers, ensure the security of these.

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

Creditors and Financial Entities: Netboss Comunicaciones S.L. must comply with the financing conditions established contractually with this type of entities, mainly, to make the loan repayment payments in the established times.

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

4. LEADERSHIP

4.1. Management commitment

The present Security Policy is a clear, manifest and public line of action of Netboss Comunicaciones S.L., so the management expresses its full support to it and is committed to maintain the guidelines set out in this document. Likewise, it will publish and deliver to all its employees and in the most appropriate way the Policies and Regulations, so that everyone knows the objective established by the Security Committee, the policies, principles and rules adopted and their importance for the security of the company, the general and specific responsibilities in security matters of each member of the company and other references to documentation that may be useful.

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

- It is involved in communicating to the organization the importance of meeting customer, legal and regulatory requirements.
- Establishes the Information Security Policy.
- It establishes the system's Objectives, as well as the planning, as described in this Security Policy.

- Conducts Management System reviews
- The availability of resources is ensured.

4.2. Information Security Policy Requirements

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

- It is appropriate to the purpose of the organization and the nature of the activities, products or services.
- It expressly includes a commitment to comply with applicable laws, regulations and other requirements deemed appropriate.
- It provides a frame of reference for establishing and reviewing the objectives of the Management System.
- It is communicated and understood by the appropriate levels of the organization.
- It is reviewed for continuing suitability.
- The review shall be carried out periodically, at least in the Management Review of the Management System (as established in this Safety Policy), and, extraordinarily, whenever the Management considers it necessary.

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

4.3. Information Security Policy

The information security policies are included in the "Security Principles" section.

4.4. Roles, responsibilities and authorities in the organization

4.4.1. Security Committee

The Security Committee coordinates the information security in Netboss Comunicaciones S.L. and is formed by:

- Company management.
- Responsible for the information.
- Responsible for services.
- Security Manager.
- Systems manager.

The Safety Committee shall meet at least once a year.

4.4.2. Roles: Functions and Responsibilities

In order to efficiently manage the Information Security, each department of Netboss Comunicaciones S.L. shall comply with the corresponding rules and procedures. All these rules and procedures will be ratified by the Management.

The members of the Security Committee are as follows:

- **Responsible for the Information Service:** Company management: CEO, general management or whoever delegates. The CEO or general management is Jose María Fernández de Arco or Sol Rojo Vallejo.
- **Responsible for the information:** systems director. Rubén Fernández Crespo
- **Security Manager:** Systems Director. Rubén Fernández Crespo
- **Responsible for the system:** responsible for the management system. Sol Rojo Vallejo

The roles and responsibilities are detailed below:

4.4.2.1. Address

The Management of Netboss Comunicaciones S.L. is committed to respond for the obligations inherent to the information security and to protect its information assets implementing the most appropriate security measures to achieve it in an effective way with the available resources.

4.4.2.2. Responsible for the information

He will be responsible for:

- The risk of all information.
- Ensure the proper use of information and, therefore, its protection.
- Any error or negligence leading to a confidentiality or integrity incident.
- Establish security information requirements.
- Determine the levels of information security.

4.4.2.3. Responsible for Services

He will be responsible for:

- The risk of all Services.
- Establish the security requirements of the service, including interoperability, accessibility and availability requirements.
- Determine the security levels of the services.

4.4.2.4. Security Manager

- He is responsible for Information Security (including GDPR files).
- It is the Asset Owner of all the company's assets as far as ISO 27001 is concerned. The asset inventory may specify an Asset Manager, to whom the Asset Owner delegates decision making with respect to the asset.
- He is responsible for the management and maintenance of the Management System.
- Ensures that the processes of the Management System are established, implemented and maintained in accordance with the requirements of the applicable standards.
- It informs the Management of the operation and effectiveness of the system so that it can carry out the review, and as a basis for the improvement of the company's management.
- Promotes awareness of customer requirements for Information Security at all levels of the organization.
- Collaborates with management in the definition and implementation of policies and regulations so that they are a true reflection of the company's strategy.
- Plans, schedules and participates, when appropriate, in internal and external audits.
- Controls the preparation, updating, approval and distribution of the Management System documentation.
- Acts as an interlocutor with external parties (customers, suppliers, management, and other interested parties) on aspects of the management system.
- Controls the execution and effectiveness of the actions taken to prevent and manage nonconformities, and assesses the actions to be taken following the communication of a suggestion for improvement.

4.4.2.5. System Manager

He will be responsible for:

- Risk of all assets, with the exception of essential assets (Services and Information).
- Develop, operate and maintain the Information System throughout its life cycle, from its specifications, installation and verification of its correct functioning.
- Define the typology and management system of the Information System, establishing the criteria for its use and the services available in it.
- Ensure that specific security measures are properly integrated into the overall security framework.

- Administration and management of user accounts.
- Ensure that only those authorized to have access have access to it.
- Ensure that the systems have the availability levels required by the Organization.
- Include applicable safety aspects in the requirements for new developments.

4.4.2.6. Risk Owner

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

- Participate in the development of the risk analysis and assessment carried out at least annually.
- Verify compliance with acceptable risk levels and collaborate in the approval of these (that affect it), as well as the management of risks associated with information assets and the risks for which it is responsible.
- Ensure that staff report any security breach or misuse of information or systems to you immediately. The risk owner must in turn inform the security manager to deal with the incident.
- Inform the Security Manager when there are changes in the personnel, the organization, or the rest of the information assets, which may imply a revision or update of the risk analysis, or of the assigned access permissions.

4.4.2.7. Asset Owner

The owner of an asset, meaning the person responsible for the asset, shall have the following responsibilities:

- Define whether the asset is affected by the Data Protection Law and apply the corresponding procedures, if applicable.
- Ensure that the software being used is licensed.
- Define who can access the information, how and when, according to the classification of the information and the function to be performed.
- Ensure that the asset is properly maintained.
- Ensure that staff report any security breach or misuse of information or systems to you immediately. The asset owner should in turn inform the security manager to deal with the incident.
- Ensure that staff are adequately trained, know and understand the Safety Policy and implement safety guidelines.
- Ensure that media and equipment containing information are disposed of as required.

- Implement the necessary security measures in your area to avoid fraud, theft or interruption of services.
- Maintain up-to-date documentation of all critical functions to ensure continuity of operations in case someone is unavailable.
- Inform the Security Manager when personnel changes occur that affect access to information or systems (change of function or department, leaving the company) so that access permissions can be modified appropriately.
- 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 their work.
- Ensure that your actions do not result in any security breaches.
- Inform the asset owner of any security incident, real or suspected, that it detects.

4.4.3. Designation Procedure of responsible

The Safety Officer shall be appointed by Management on the proposal of the Safety Committee. The appointment will be reviewed every 2 years or when the position becomes vacant.

Management shall also designate the person responsible for the System, specifying his/her functions and responsibilities within the framework established by this Policy.

4.4.4. Communication

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

- Decide and respond to staff concerns on Management System issues.
- Communication between the different operational areas of the organization, in order to follow the evolution of the operational processes of the Management System and to coordinate and unify action criteria.
- Communication at the area level, in order to share among its members the knowledge and best practices acquired from experience during the development of the corresponding processes.

- Receive, document and respond to relevant communications from the organization's stakeholders, as well as ensure internal communication between the various levels and functions of the organization.

To ensure such communication, we proceed as follows:

- The Safety Manager, through periodic departmental meetings with personnel, internal e-mail, etc., is responsible for communicating the Policies, objectives, goals and evolution of the Management System in general and of the management of customer requirements in particular. These communications will take place whenever the person in charge considers it appropriate and, in any case, after system reviews and audits, in order to disseminate the results and decisions of a general and specific nature arising from these activities.
- To ensure that timely and urgent information is communicated to the personnel concerned, the organization has internal communication tools: e-mail, slack, telephones, etc., which have a sender and one or more recipients, and are used to communicate information concerning, for example, changes in an order that had already been communicated to the personnel concerned, a new person joining the organization, the reception of a visit to the organization, etc.

A Communication Plan has been defined, detailing the communication channels between the different 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 actions must be developed and governed.

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

- Achieve Security Objectives.
- Ensure that organizational changes are carried out in a controlled manner and that the Management System maintains its integrity during these changes.
- Management Planning is carried out on an ordinary basis at the System Review Meeting, and on an extraordinary basis whenever Management so decides, being documented, in any case, in the final minutes of these meetings.

4.5.2. Planning result.

As a result of the planning, the 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:

- Approved objectives and goals.
- The assignment of responsibilities at each relevant function and level of the organization for the achievement of objectives and goals.
- The means and the timeframe in which they are to be achieved.

Objectives are measurable, established and reviewed considering safety requirements, technological options and financial, operational and business requirements, as well as those necessary to satisfy product/service requirements and the commitment to continuous improvement, customer and general stakeholder feedback.

To evaluate the degree of compliance, and to ensure the adequacy and effectiveness of the system, the objectives are reviewed periodically, and the conclusions of their follow-up are discussed at the meetings of the Safety Committee, 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 necessary resources to implement and improve the processes of the Management System, and to achieve customer satisfaction, information security and service delivery.

5.1.2. Infrastructure

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

-Work space and associated facilities.
-Equipment , hardware and software.
-Support services.

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

5.2. Persons

Netboss Comunicaciones S.L. has established, and keeps up to date, the procedure **SGI P71 Personnel Management**, which describes the criteria and associated responsibilities to ensure that those personnel who have responsibilities defined in the Management System are competent based on applicable education, training, awareness, practical skills and experience.
Security linked to personnel is essential to reduce the risks of human error, theft, fraud or misuse of facilities and services.

5.3. Communication

A Communication Plan shall be developed to establish the communication channels between the different stakeholders of the system (see document **SGI D74 Communication Plan)**.

5.4. Documented information

In order to develop this Management System, we have a documentary structure composed of:

- Safety Policy, the present policy: document where the bases of the company's Management System are established.
- Regulations, documentation defining the uses permitted or prohibited in the organization.
- Procedures: describe the activities required to implement the Management System in order to comply with the requirements of any of the applicable standards.
- Documents: any information in any type of support of the integrated management system.

The different documents are of adequate length to ensure the effective operation of the system and the organization and control of the processes, depending on the complexity of the process, the interaction of the different processes and the competence of the personnel involved.

5.4.1. Control of Management System documentation

Netboss Comunicaciones S.L. has established, and keeps up to date, the management procedure of the ISMS where it is described how the control of the documentation of the System must be carried out, where the criteria and responsibilities associated to the control of the necessary documents for the operation of the Management System are described.

5.4.2. System Documentation

ISO 27001	ENS	System Document
4. organizational context	org.1 Security policy	ISMS D51 01 Security Policy

ISO 27001	ENS	System Document
4.1 Understanding of the organization and its context		ISMS D51 01 Security Policy SGI P61 Risk Management and Analysis Risk management
4.2 Understanding stakeholder needs and expectations		ISMS D51 01 Security Policy
4.3 Determination of the scope of the information security management system		ISMS D51 01 Security Policy ISMSI D613 01 Applicability Document
4.4 Information security management system		ISMS D51 01 Security Policy
5. Leadership		ISMS D51 01 Security Policy
5.1 Leadership and commitment		ISMS D51 01 Security Policy SGI D3 Integrated Management System Manual
5.2 Policy	org.1 Security policy	ISMS D51 01 Security Policy
5.3 Roles, responsibilities and authorities in the organization	org.1 Security policy	ISMS D51 01 Security Policy
6. Planning		ISMSI D613 01 Applicability Document SGS P843 Capacity Plan SGI P61 Risk Management and Analysis 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 Management and Analysis 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		ISMS D61 Risk Categorization SGI P61 Risk Management and Analysis 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
7.3 Awareness	mp.per.3 Awareness	SGI P71 Personnel Management SGI D10 03 Improvement Plan

ISO 27001	ENS	System Document
7.4 Communication		ISMS D51 01 Security Policy SGI D74 Communication plan
7.5 Documented information		ISMS D51 01 Security Policy SGI D3 ISO integrated management system manual SGI P71 Personnel Management
8. Operation		SGI D3 ISO integrated management system manual
8.1 Operational planning and control		ISMS P858 Logical Security ISMS P854 Access Control ISMSI P861 Incident Management ISMS P855 Physical Security SGI P75 02 Protection of Personal Data SGI P75 01 Information Protection SGI P83 Software Development SGI P84 01 Supplier management
8.2 Assessment of information security risks	op.pl.1 Risk analysis	SGI P61 Risk Management and Analysis SGI P61-01 Risk Analysis and Management Report P61 Risk Analysis and Management
8.3 Treatment of information security risks	op.pl.1 Risk analysis	SGI P61 Risk Management and Analysis 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 D3 ISO integrated management system manual
9.2 Internal audit		SGI D3 ISO integrated management system manual
9.3 Management review		SGI D3 ISO integrated management system manual
10. Improve		SGI D3 ISO integrated management system manual
10.1 Nonconformities and corrective actions		SGI D3 ISO integrated management system manual ISMSI P861 Incident Management
10.2 Continuous improvement		SGI D3 ISO integrated management system manual

6. OPERATION

6.1. Operational planning and control

During the planning of the service delivery, the following points are determined when appropriate:

- Safety objectives and service requirements.

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

6.2. Treatment of information security risks

Analyzing potential risks and developing a strategy to manage them properly is paramount for Netboss Comunicaciones S.L. because only if the security status is known with rational evidence, appropriate decisions can be taken to solve the risks that arise.

Each asset has a valuation in terms of Availability, Integrity, Confidentiality, Authenticity and Traceability, which will be carried out using the criteria detailed in the ISMS document **D61 risk categorization.**

The MAGERIT methodology ("Methodology for the Analysis and Management of Information Systems Risks"), developed by the Superior Council of Electronic Administration, was used to perform the risk analysis.

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

MAGERIT covers risk analysis and treatment activities by 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 risks identified, so that the damage they may cause is eliminated or, if this is not possible, reduced as much as possible.

Risk management is the comprehensive process of dealing with risks discovered during the analysis.

6.2.1. Risk Analysis Process

- Netboss Comunicaciones S.L. assets 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. If we estimate the probability of the threat, we can conclude the risk in the system, or the loss to which it is exposed.
- Degradation and probability rate the vulnerability of the system to a threat.

6.2.2. Risk Management Process

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

The following strategies can be chosen to mitigate the risk:

- Assume the risk: accept the risk and do not implement controls to reduce or eliminate it.
- Risk avoidance: eliminating the cause or consequence of the risk.
- Reduce risk: limit risk by implementing controls that reduce the impact.
- Transfer the risk: pass the risk to others, such as an insurer.

Safeguards will be deployed to address threats.

The safeguards mitigate the impact and risk values leaving them reduced to residual values, which will be assumed by the person responsible for the information or the person responsible for the service.

The corresponding Applicability Document will specify for each ISO 27001 or ENS control, whether it is applicable or not and the reason for this decision.

The risks and controls adopted following the risk analysis must be reviewed annually, as well as whenever circumstances make it advisable. This shall be considered as a further part of safety 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.

In the event that a deviation is detected with respect to the planned results in the indicators, the safety manager must open a "non-conformity" in order to analyze the cause of the deviation and 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 Manager shall review the Policies annually or when significant changes make it advisable, and shall resubmit them for approval by the Management. The reviews will verify the effectiveness of the policies, assessing the origin, number and impact of the incidents recorded since the implementation of the ISMS, the cost and impact of the controls established and the improvement measures adopted in the company and the effects of technological changes. These reviews will include the information systems, the system suppliers, the owners of information and information assets, the users and also the Management.

The Management Committee of Netboss Comunicaciones S.L. will ultimately be in charge of approving the necessary modifications to the text when a change occurs that affects the assets originally evaluated and the risk situations established.

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

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

7.3. Management Review

Management conducts reviews of its Information Security Management System to ensure its continued consistency, adequacy and efficiency. The review performed evaluates the need for changes to the Management System, including policy, objectives and other elements in view of the results of the system audit, changing circumstances and the commitment to continual improvement. All this is set out in the SGI D3 Procedure Integrated Management System Manual.

With the results of the Review, the 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 do so, it relies on 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 nonconformities in order to prevent their recurrence, the procedure SGI D3 Integrated Management System Manual has been established and kept up to date, where the criteria and responsibilities associated with:

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

9. SAFETY PRINCIPLES

9.1. Asset Management

9.1.1. Liabilities associated with assets

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

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

9.1.2. Classification of information

The classification of the information will be according to the following scale:

Confidential	Information to which only certain individuals or departments within the organization should have access. If leaked to third parties, it could have serious consequences for the organization.
Internal Use	Information that should only be accessible to the organization's personnel. If leaked to third parties, it could have consequences for the organization.
Public	Information without any need to restrict access. If leaked to third parties, there would be no consequences for the organization.

There will be a list of the information in Netboss Comunicaciones S.L. with the corresponding classification (Confidential/Internal Use/Public). Netboss Comunicaciones S.L. staff will be aware of this classification so that they know at all times the type of information they use, without the need to establish a marking of this, thus not revealing to external sources the classification of information. The destruction of this information will be carried out by the person in charge of the asset following the guidelines approved by the Security Manager and with his collaboration if necessary.

9.2. Human Resources Management Security

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

The recruitment of personnel goes through a selection process in which references and background checks should be conducted whenever possible.

The terms and conditions of the employment relationship shall reflect the employee's responsibilities for information security. This responsibility shall continue for a set period of time after termination of the contract.

A confidentiality agreement will be required to be signed by all employees to prevent disclosure of secret information.

All safety policies and procedures shall be regularly communicated to all workers and third party users as appropriate. Seminars shall be conducted on a regular basis to ensure that personnel are aware of the safety processes and tasks they are required to perform.

Employees who violate safety rules may be sanctioned by a disciplinary process in accordance with the general agreement.

When the employment or contractual relationship with employees or external personnel is terminated, they will have their access permissions to the facilities and information withdrawn and will be asked to return any information or equipment given to them for the performance of the work.

9.3. Physical and Environmental Safety

For logical security to be effective, it is essential that Netboss Comunicaciones S.L. facilities maintain proper 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 so that only authorized persons have access to the facilities.
- All Netboss Comunicaciones S.L. offices have the necessary physical barriers to secure the resources they house.
- The locations where the server and cabling are located shall be locked and only authorized persons and service providers shall have access when accompanied by an authorized person.
- Windows and doors must remain closed when the premises are empty.
- Netboss Comunicaciones S.L. facilities are equipped with fire extinguishing devices marked by the current legislation in this area. In this sense, fire extinguishers and emergency exits are properly marked.
- Personnel are expressly prohibited from eating and drinking near servers and computer equipment. Likewise, special care shall be taken with the handling of any product that may be spilled on information assets.
- In order to prevent water leaks and flooding, it will be necessary to periodically check the faucets, toilets and other installations that may cause this type of damage.

9.3.2. Equipment safety

- IT equipment is an important asset on which the continuity of the organization's activities depends, so it must be adequately and effectively protected.
- Both user workstations and servers are protected against possible power failures or other electrical

anomalies by the installation of uninterruptible power supplies.

- The equipment must be properly maintained to ensure its correct operation and perfect condition in order to maintain the confidentiality, integrity and above all the availability of the information. To this end, they must be subjected to the revisions recommended by the supplier. Only duly authorized personnel will be able to access the equipment to proceed to its repair. It will also be necessary to adopt the necessary precautionary measures in case the equipment must leave the facilities for maintenance.
- The disposal of equipment shall only be carried out by the Safety Officer or personnel delegated by him/her.

9.4. Communications and operations management

9.4.1. Operating Procedures and Responsibilities

Netboss Comunicaciones S.L. will control the access to the services in internal and external networks and will make sure that the users do not put these services at risk. For this purpose, it shall establish the appropriate interfaces between the Netboss Comunicaciones S.L. network and other networks, the appropriate authentication mechanisms for users and equipment, and the accesses for each user of the information system.

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

All workers authorized to handle automated information must be registered as users of the information system. Each time they access the information system, they must validate themselves with their user name, which shall be unique and non-transferable, and their personal password.

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

9.4.2. Management of Services Provided by Third Parties

Netboss Comunicaciones S.L. when hiring an external service to manage information assets introduces new vulnerabilities in the process, since the resources are exposed to possible damages, losses or information leaks. Therefore, it will be necessary to take a series of precautions to ensure the perfect use of Netboss Comunicaciones S.L. information.

Before contracting an external service for information management, Netboss Comunicaciones S.L. will identify the risks that this situation entails and will draw up an agreement in which the following issues are addressed: which applications are maintained in Netboss Comunicaciones S.L. because of its special criticality, the approval of the owners of the application, what implications the contract has for the business continuity plans, the security standards and how their effectiveness will be measured, who are the responsible and what special procedures will be followed to monitor the important security activities, who and how will handle the security incidents and through what procedures Netboss Comunicaciones S.L. will be informed of those incidents.

9.4.3. Protection against malicious code and mobile code

It is strictly forbidden the installation of other software that is not allowed and necessary for the development of the work by Netboss Comunicaciones S.L. staff.

All software acquired by the organization, whether by purchase, donation or assignment, is the property of the institution and will maintain the rights conferred by the intellectual property law, monitoring the different types of licenses.

Any software that needs to be installed to work over the Network must be evaluated by Management.

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

9.4.4. Backups

Data should be stored in a network directory to ensure that it is backed up regularly.

There shall be procedures for making backup copies that shall be archived for data recovery in the event of an incident. These copies shall be clearly identified and stored in a secure location, preferably outside the organization's premises.

Procedures will also be developed to recover data from backup copies. It must be periodically ensured that the information is correctly stored and that a minimum level of service can be recovered if necessary.

If information is corrupted in operation, the software, hardware and communications involved must be checked before using the backups to ensure that the information contained in the backups cannot be corrupted as well.

9.4.5. Network security management

All computer equipment (workstations and server...) that are or will be connected to the network, or those that are independently owned by Netboss Comunicaciones S.L. must be subject to the rules and installation procedures issued by the IT department and that have been previously ratified by the Management.

The network elements (switch, router, etc.) shall be kept out of the access of unauthorized personnel to avoid malicious uses that could jeopardize the security of the system.

9.4.6. Support Management

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

Media (both paper and logical) containing sensitive information must be kept in locked drawers or cabinets. When an authorized person must use it to carry out some management related to the work of the company, he/she shall be responsible for the proper care of the media. They shall not leave them on their desk when they leave their workstation, nor shall they place them in any other place where an unauthorized person could see them or take possession of them.

Reusable media whose information is no longer needed should be deleted, provided that the necessary authorization is obtained. This disposal should be done in a secure manner so that the data it contains is not leaked to others. Some destruction procedures that are considered appropriate are incineration, shredding or emptying of the media to be used in another application within Netboss Comunicaciones S.L.

It will always be necessary to record the disposal of media containing sensitive information to maintain an audit trail.

9.4.7. Information Exchange

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

9.4.8. Follow-up

As deemed necessary, mechanisms will be established to detect unauthorized information processing activities. This will involve performing tasks to carry out checks and inspections of system records and activities to test the efficiency of data security and data integrity procedures, to ensure compliance with 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

The information must be protected against unauthorized access.

Each department or area manager shall define the information access needs at two levels, for the department or area as a whole and for each user within the whole. Access will only be provided to the information necessary for the work to be carried out.

In the event that visitors or unauthorized personnel access Netboss Comunicaciones S.L. facilities or information, they must always be accompanied by a responsible member of Netboss Comunicaciones S.L. who will control at all times that the security of the resources is guaranteed.

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 associated to a profile, according to the tasks he/she performs in the organization, defined by his/her direct manager. Each of these profiles will have certain permissions and will be restricted in their access to information and systems that are not necessary for the competencies of their work.

9.5.3. *User responsibilities*

Staff workstations should be kept clear of paper and other information storage media to reduce the risk of unauthorized access and other possible damage. These should be stored in suitable enclosed spaces, especially outside working hours.

Similarly, it is necessary to configure the computer equipment so that it is locked when the user is not at work, so that a password must be entered to access the data stored in the terminal.

Mail entry and exit points, fax machines and printers that are not attended by a Netboss Comunicaciones S.L. person must also be protected.

9.5.4. *Network access control*

Access to the network, systems, applications or information will not be allowed to any user who is not formally authorized to do so.

In the case of service providers or external entities, who 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 person in charge of security will control the registration and deregistration of all users.

9.6. Incident management tes

Any employee who suspects or observes a security incident, whether physical (fire, water, etc.), software or systems (virus, data disappearance, etc.) or support services (communications, electricity, etc.) must immediately inform the Security Manager so that he/she can take the appropriate measures and record the incident.

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

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

9.7. Business continuity

It is essential for Netboss Comunicaciones S.L. to establish the guidelines to be followed in the event of an interruption of business activities due to serious security failures or disasters of any kind.

To ensure business continuity in these cases, Netboss Comunicaciones S.L. will establish contingency plans that allow the recovery of activities at least at a minimum level within a reasonable period of time. The business continuity management will include, therefore, several controls for the identification and reduction of risks and a procedure that limits the harmful consequences of the same and ensures the resumption of essential activities in the shortest possible time.

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

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

9.8. Acceptable Use Policy

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

- The creation or transmission of material in violation of data protection or intellectual property laws.
- Install, modify or change the configuration of software systems (only system administrators are authorized to do so).
- Use of the Internet for personal purposes (including personal Web-based e-mail) shall be limited to authorized break times. Any personal electronic transactions are at the user's own risk.
- Deliberately facilitating access to facilities or services to unauthorized persons.
- Wasting network or system resources in a premeditated manner.
- Corrupt or destroy other users' data or intentionally violate their privacy.
- Intentionally introducing viruses or other forms of malicious software. Before using any information storage media, check that it is free of viruses or similar.
- Voluntarily disclose passwords and means of access.
- Use the equipment for personal gain.
- The creation, use or transmission of material that is offensive, obscene or likely to cause discomfort or offense.
- Sending very large e-mail messages or to a very large group of people (which can saturate

communications).
- Failure to verify that emails are virus-free.

Likewise, users must take into account the following security measures during the processing of information and the use of IT systems:

- Any person who suspects or observes a security incident, whether physical (fire, water, etc.), software or systems (virus, disappearance of data, etc.) or support services (communications, electricity, etc.) must immediately notify the Security Manager so that he/she can take the appropriate measures and record the incident.
- Each user's computer equipment will be under the responsibility of an authorized user who will try to protect, to the best of their ability, the confidentiality of the company's information and, especially of the personal data to which they have access, against unauthorized disclosure or any other manipulation or misuse.
- When the person responsible for a computer equipment leaves it temporarily, he/she shall leave it in a state that prevents the display of protected data, locking the user and preventing the use of the workstation. Resumption of work shall involve deactivating the protective screen by entering the corresponding password. If the abandonment of the equipment should occur due to the end of his work shift, the user will proceed to the complete closing of the system session.
- All documents containing company information should be removed from printers and other output peripherals as they are printed.
- No user may use removable devices (CD, DVD, USB, etc.) or store information on them without prior authorization from the Security Manager.
- The 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.
- The media containing information shall be kept in a safe and locked place, or in rooms, offices, ... with restricted access, when not in use, especially outside working hours.
- No user may install or execute programs that could interfere with the work of other users, or damage or alter any of the computer resources. Under no circumstances may they install illegal or irregular copies of programs, or delete any of the legally installed programs.
- It is strictly forbidden to modify the configuration of any software, whether operating system or applications, established by default in the computer equipment by the person responsible for security, without prior authorization.
- The use of e-mail and the Internet should be limited to job-related functions.
- Do not reply to fake e-mails or chain e-mails to prevent your e-mail address from being disseminated. Do not open suspicious attachments from strangers or unsolicited attachments.
- If viruses are detected in files or e-mails received or while surfing the Internet, you must inform the Security Manager.
- Passwords will be assigned to all system users as a means of validating their identity. The procedure for assigning passwords is done through personal delivery by the IT manager, who is responsible

for communicating the user and password for access to the systems.

- The password will be composed of a minimum of 12 characters, (It must have at least 3 of these 4 characteristics. Uppercase, lowercase, numbers or special characters) and must not be revealed under any circumstances, nor must it be kept in writing or in view of third parties.
- It is advisable to change passwords on a quarterly basis. It is also necessary for the equipment to have screen protectors that are activated after five minutes of inactivity, and an unlocking password is required.
- The password must not contain the account identifier or user name, or any other personal information that is easy to know (birthdays, names of children, spouses, etc.). Nor should it contain a series of letters arranged adjacent 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 one of them is exposed, all other accounts protected by the same password should also be considered at risk.
- Do not share passwords on the Internet, by e-mail or by telephone. In particular, be wary of any e-mail message asking you for your password or telling you to visit a Web site to check your password.
- If a user has a well-founded suspicion that his/her authorized access is being or may be used by another person, he/she will be obliged to change his/her password by contacting the Security or IT manager to report the incident.
- No authorized access of another user may be used, even if authorized by the owner.
- No user should attempt to access restricted areas of their own or third parties' information systems, other than those assigned to them.

The laptops and cell phones will be assigned by Netboss Comunicaciones S.L. There will be an updated inventory of the laptops and cell phones. Netboss Comunicaciones S.L. will be the unit in charge of managing this inventory.

- This type of devices will be under the custody of the user who uses them or the responsible of Netboss Comunicaciones S.L. Both will have to adopt the necessary measures to avoid damages or theft, as well as the access to them by unauthorized persons. The subtraction of this equipment must be immediately reported to Netboss Comunicaciones S.L. for the adoption of the corresponding measures and for the purpose of inventory deletion.
- Portable and mobile equipment should be used only for institutional purposes, especially when used outside Netboss Comunicaciones S.L. facilities.
- The users of this equipment will be responsible for not being used by third parties outside Netboss Comunicaciones S.L. or not authorized to do so.
- Mobile devices will require user authentication for access to mobile devices and installed applications.
- In general, laptops should not be connected directly to external networks (including the user's network or Internet access at home). In duly justified cases and previously authorized by Netboss Comunicaciones S.L., alternative connections may be used, observing strict security measures

regarding Internet browsing and the rest of the precepts of these General Regulations that may be applicable.

- Connections to open wifi networks, such as those provided in airports, hospitals, shopping centers, conferences, congresses... are prohibited, as these networks are not secure and information can be extracted from the communications established during the connection.
- Additional software will be used to protect the devices through the use of antivirus systems, as well as actions such as remote location and deletion in the event of loss of the devices.