Policy

Information Security Policy

Approved by:

Miguel Angel Acero

VP Operations

Ramon Viñas, 4, 08930 Sant Adrià de Besòs, Spain – NIF ESA66087420
AFR-IX telecom has an ISMS certified in accordance with UNE-ISO/IEC 27001:2014 standard.

Signature control

Created by	Reviewed by	Approved by
CISO	CIO	Miguel Angel Acero **VP Operations**

Archive	Update	Distribution List	Access Level
Process	SGSI	All employes	***INTERNAL USE:*** *Internal use for AFR-IX Telecom*

Version and change control

Version	Date	Modification	Section
V1	06/07/2020	Creation of Document	All pages
V2	15/07/2020	Regulatory framework update	All pages
V3	28/04/2022	Normative framework update	All pages
V4	23/02/2023	Change of format and Nomenclature Change of Responsibilities	All pages Pg 9
V5	22/03/2024	Change in the content of the document in order to simplify it.	All pages

Table of Contents

1 Introduction....4
2 Objective....4
3 Scope....4
4 Responsibilities....4
5 Description....5
5.1 Information security principles....5
5.2 Implementation of an Information Security Management System....5
5.3 ISMS Review and continuous improvement by achieving information security objectives....6
5.4 Corporate commitment....6
6 References....7
7 Confidentiality and ownership....8

1 Introduction

- AFR-IX carries out its work by providing quality Internet points of access and digital communications services with added value. To carry out this purpose, it carries out business processes that require the management of information by means of computer services that are supported and integrated in an information system.
- AFR-IX is aware of the need to ensure that the information it manages, as well as the services it handles, must receive adequate protection to comply with legal compliance requirements, prevent unauthorized access to information and personal data, preserve its integrity and ensure that the business processes and the information they manage will be available when needed.

2 Objective

The purpose of this document is to establish the general guidelines that determine AFR-IX's commitment to ensure the protection of the services, information, and personal identifiable data (PII) that are managed in its business processes.

3 Scope

This policy applies both to people and organizations that, in one way or another, interact with AFR-IX´s information system, including suppliers, collaborators or any other interested parties.

4 Responsibilities

This policy involves and must be accomplished by all personnel of AFR-IX and by any other stakeholder that interacts with its information system.

CISO:

- Responsible for notifying this policy to the staff of the entity and any changes in it, as well as coordinating the actions of implementation, maintenance and improvement of the ISMS of the entity, and its audits

5 Description

5.1 Information security principles

The fundamental principles that will govern the protection of the security of information in AFR-IX will be the following:

- End-to-end security. Requiring the inclusion and coordination of all personal, material, technical, legal, and organizational elements related to AFR-IX's information system.
- Risk-based security. Analyzing the impacts and probabilities of risks that may threaten the information system and taking measures to address them at levels that do not affect the achievement of business objectives.
- Monitoring, surveillance, detection, response, and restoration measures. Establishing tools and processes that continuously monitor the operation of the information system, detect anomalies and threats, prevent their materialization and, if they finally occur, make it possible to recover the affected information and return to the initial situation.
- Training and awareness. Selecting people with the right skills to intervene in the system's processes, training them to improve these skills and making the whole company aware of the need for a proactive stance in defense of the security of information and services.
- Information Technologies management services. Implementing management processes to appropriately regulate all the security activities that frame and protect the information system in a formal, coherent, and documented manner.
- Legal Compliance. Analyzing in detail the legal framework in which the company's activities are framed and establishing the necessary measures to comply with the corresponding legal obligations.
- Continuous improvement. Providing the system with mechanisms for regular review of its operation, analyzing measures to correct any dysfunctions that arise and actively looking for opportunities to improve its design and operation.

5.2 Implementation of an Information Security Management System

To comply with the above principles, AFR-IX has decided to implement an Information Security Management System (ISMS) based on a risk-management approach. Risks are identified by analyzing the vulnerabilities the information system suffers from and, after evaluating the impact and probability of those risks to materialize, establish and apply the appropriate safeguards to mitigate them.

This risk assessment takes into consideration the interested parties, the internal and external factors that condition the AFR-IX´s information system, and the legal framework the company is embedded on.

To assure the coherence, repeatability, and improvement of all the processes required from the AFR-IX´s Information Security Management System, they will be appropriately documented in a series of policies and procedures that will develop in detail the main guidelines of this security policy. These policies and procedures will be reviewed periodically.

For the operation of the Security and Privacy Management System to fulfill its purpose and to meet its objectives, the organizational structure of AFR-IX will have the required positions, as well as specific applicable roles, assigning them the responsibilities that are necessary to properly govern the system. In this context an Information Security Committee will be created as the collegiate transversal body within AFR-IX for the supervision and management of the Information Security Management System.

All AFR-IX employees will be provided with appropriate awareness on the security risks them may encounter and will receive appropriate training according to their relationship with the ISMS.

5.3 ISMS Review and continuous improvement by achieving information security objectives

AFR-IX is committed to reviewing and improve the Information Security Management System by establishing information security objectives with the purpose to mitigate a risk or improve the AFR-IX security posture. Its achievement will reflect the principle of continuous improvement of information security and will require the accomplishment of a task.

These information security objectives will be obtained from the reviews that are carried out regularly to evaluate the system's processes, from non-conformities arising from internal and external audits that are scheduled, as well as from the initiative of all the ISMS stakeholders when they perceive dysfunctions or opportunities for improvement.

Information security objectives will have designated owners, sufficient resources, indicators for achievement, and plausible timelines for completion. Its development and implementation will be reviewed frequently.

5.4 Corporate commitment

Achieving the objectives of the information security management system requires from AFR-IX a complete commitment to ensure its execution and the improvement of the processes and activities that it entails. This commitment will be materialized by:

- The delivery and communication of these guidelines to all the company's employees and to those external people and organizations that require their knowledge. This document will be published in a medium accessible to all those involved and will be reviewed periodically. This communication will be complemented by internal awareness-raising actions that facilitate the integration of this system into AFR-IX's business objectives.
- The provision of enough resources to accomplish the ISMS purpose.
- The allocation of delegated authority to appropriate personnel to accomplish its responsibilities to manage the ISMS.

6 References

7 Confidentiality and ownership

AFR-IX telecom, an infrastructure and telecommunications operator, incorporated and registered in Spain with NIF A66087420 and registered office at Calle Ramon Viñas 4, 08930 Sant Adrià de Besòs, Barcelona, is the owner this document and it should be treated as confidential. Confidential information may not be reproduced by any means or in any format by the Recipient without the express prior written authorization of AFR-IX telecom. In the event that the Recipient is authorized by AFR-IX telecom to reproduce all or part of the Confidential Information, all reproductions, whether total or partial and whatever the format in which they are recorded, must make express mention of AFR-IX telecom's intellectual property rights over the information contained therein, bearing confidentiality notices and maintaining the legends contained in the original Information, unless otherwise provided for in writing.