AFR-IX telecom

INFORMATION SECURITY POLICY

April 2022

Index

1 General Information

1.1 Purpose

The purpose of this policy is to establish the commitment of **AFR-IX Telecom management**, represented by its Security Representative, with information security and the protection of information assets necessary for the performance of the functions described in the scope, thus enabling the achievement of its business and strategic objectives.

This commitment is materialized through the implementation and maintenance of an Information Security Management System (ISMS) in accordance with the international standard ISO/IEC 27001, and with the extension of the ISO 27011 so as to better adapt the requirements to the operations of AFR-IX as a telecommunications provider.

The main objective of the Information Security Policy is to guarantee the security of the information and the continuous provision of the AFR-IX services, acting preventively, supervising the activity and reacting promptly to any incidents that may occur.

This Policy should provide the basis for access, use, custody and safeguarding of the information assets used by AFR-IX to carry out its functions, under guarantees of security, in all its different dimensions:

- Availability: property or characteristic of the assets consisting of access to them by authorized entities or processes when required.
- Integrity: property or characteristic consisting of the information asset not being altered in an unauthorized manner.
- Confidentiality: property or characteristic that the information is neither made available nor disclosed to unauthorized individuals, entities or processes.

Under these premises, the specific objectives of Information Security at AFR-IX will be

- To ensure the security of information, in the different dimensions described above.
- To formally manage security, based on risk analysis processes.
- To develop, maintain and test the availability and business continuity plans defined for the various services offered by the organization.
- To carry out an adequate management of incidents that affect the security of the information.
- Keep all personnel informed about security requirements and disseminate good practices for the safe handling of information.
- To provide the levels of security agreed with third parties when information assets are shared or transferred.
- Comply with current regulations and standards.

1.2 Scope

This Security Policy will be applied to all areas, departments and companies that make up AFR-IX and to its information systems and assets:

- To all departments, both their managers and employees.
- To suppliers, clients or any other third party that has access to the organization's information or systems.
- To databases, electronic and paper files, treatments, equipment, supports, programs and systems.
- To the information generated, processed and stored, regardless of its support and format, used in operational or administrative tasks

1.3 Distribution

Approved by AFR-IX's management, this policy must be accessible to all affected persons and organizations within the scope of the ISMS, through the appropriate channels. Similarly, the Policy will be accessible to any interested stakeholder or competent body that formally requests it.

2 Normative Framework

The control of the regulations and legislation implementing this security policy is managed by the specific compliance and legal area. More information can be found in 220330 - PR17 - Identification of Applicable Legislation

3 Management Commitment

AFR-IX's management is committed to facilitating and providing the necessary resources for the establishment, implementation, maintenance and improvement of the company's ISMS, as well as demonstrating leadership and commitment to it through the next responsibilities:

- Ensuring that this policy and the objectives of information security are established and that they are compatible with AFR-IX's strategy.
- Ensuring that the applicable requirements of the ISMS are integrated into the company's processes.
- To ensure that the necessary resources for the ISMS are available.
- Communicate the importance of effective security management in accordance with ISMS requirements.
- Ensure that the ISMS achieve the intended results.
- Lead and support people to contribute to the effectiveness of the ISMS.
- Promote the evolution and continuous improvement.
- Support other relevant management roles, leading their areas of responsibility in information security.
- Monitoring the indicators to evaluate the result/compliance.

3.1 Information Security Objectives

Information security objectives will be set at the relevant functions and levels, focused on improvement and used as a reference framework:

- Changes in stakeholders' needs leading to an improvement in the scope of the system.
- Applicable information security requirements and the results of risk assessment and treatment to ensure confidentiality, integrity, availability, traceability and authenticity of information.
- Internal factors such as the application of organisational techniques that improve the monitoring of the processing and resolution of security incidents
- External factors such as technological advances, the application of which will improve the efficiency of risk management
- The improvement of the effectiveness of the training and awareness of the personnel working in the entity and affecting their performance in information security.

Likewise, planning for the achievement of the established information security objectives will be carried out considering the following elements:

- What is going to be done.
- The necessary resources.
- The responsible.
- Term of achievement.
- Indicators to evaluate the result/compliance.

3.2 Implementation and Improvement of the ISMS

The deployment of AFR-IX's ISMS will begin with a SWOT and a Risk Analysis, which will determine the expectations of the interested parties and the level of information security risk facing the entity and identify the security controls needed to address the risk and bring it to an acceptable level, as well as the opportunities for improvement, taking into account the internal and external issues and stakeholder requirements indicated above.

The security controls must be implemented, maintained and improved continuously, and be available as documented information, through procedures, regulations, technical instructions, manuals, etc., reviewed and approved by the Information Security Officer, together with the supervision of the Data Protection Officer and finally by the management.

This Security Policy is developed by applying the following minimum requirements, which must be included in the system documentation:

- Organization and implementation of the security process.
- Risk analysis and management.
- Personnel management.
- Authorization and access control.
- Protection of the installations.
- Acquisition of products.
- Security by default.
- System integrity and updating.
- Protection of information stored and in transit.
- Prevention against other interconnected information systems.
- Record of activity.
- Security incidents.
- Continuity of the activity.
- Continuous improvement of the security process.

The documented information of the security controls must be communicated to the personnel that works in the entity (employees and suppliers), who will have the obligation to apply it in the accomplishment of their work activities, committing themselves to the fulfilment of the requirements of the SGSI.

The documented information will be classified in public, internal and confidential, giving the appropriate use according to this classification and according to the criterion that will be established in the procedure of classification, labelling and protection of the information.

Audits will be carried out to review and verify compliance with the ISMS based on ISO/IEC 27001 and ISO 27011, so if necessary, the personnel affected by the scope must collaborate in these, as well as in the application of corrective actions derived for continuous improvement.

3.3 Roles and Responsibilities

The following roles and responsibilities within the ISMS are set out, but not extensively:

- The Management of AFR-IX, represented by the Security Representative, will be in charge of approving the policy and will be responsible for authorizing its modifications, as well as all the documented information of the ISMS of the entity.
- The Information Security Manager will be 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.

- The Data Protection Officer (or similar) will be responsible for supervising and ensuring compliance with current regulations on data protection.
- All staff of the entity (internal and external) will be responsible for complying with this policy within their area of work, as well as applying all the documented information of the entity's ISMS in their work activities that affect their performance in information security.

3.4 Security Policy Review

This Information Security Policy will be reviewed by management whenever significant changes occur, at least once a year within the ISMS cycle.

4 Current Release and Acceptance

Release	Written by	Verified	Approver	Comments
	Date	Date	Date	
1.0	SEIDOR	ISMS Manager	Miguel Ángel Acero	Original – Release 1.0
	06/07/20	06/07/2020	06/07/2020	
1.1	SEIDOR	ISMS Manager	Miguel Ángel Acero	Release 1.1 Regulatory framework update
	15/07/20	30/10/20	30/10/20	
1.2	SEIDOR	ISMS Manager	Miguel Ángel Acero	Release 1.2 Normative framework update
	28/04/22	29/04/22	2/05/22	

This Information Security Policy will be approved by AFR-IX's management by signature and communicated to interested parties.

Management Representative Name: Miguel Angel Acero
Date: 02/05/22
Signature: