	Information security policy	Effective date 08/03/2024	
		Version	02
	Information security	Information classification	Internal use

FYCO, a proactive company focused on uniting borders, societies, and cultures through comprehensive solutions for the telecommunications sector, contributing to the technological development of Latin America and the Caribbean, is committed to maintaining an Information Security Management System that allows the preservation of the integrity, confidentiality, and availability of the company's information assets.

Scope

This document applies to all phases of the information life cycle: generation, distribution, storage, processing, transport, consultation, among others, and to the systems that process it.

It applies to the import, distribution and marketing of materials and equipment for the telecommunications and energy sectors of FYCO in all countries where it operates, that is, to all personnel, both internal and external; as well as to the people who directly or indirectly provide their professional services within and outside of it and to all information that is accessed, retained, created, processed, stored or exchanged within and outside the organization.

Objectives of the Information Security Management System

- Protect the information of suppliers, customers, employees and other stakeholders, as well as the technology used for its processing, ensuring the confidentiality, integrity and availability of the information throughout its lifecycle.
- Identify in a timely manner the information security risks associated with the organization's assets, for their appropriate treatment.
- Identify and address information security incidents, as well as vulnerabilities of the technologies implemented for the protection of the business's own information.
- To create an Information Security culture within the company, encouraging our employees, suppliers, customers, and other stakeholders to adopt best practices and secure behaviors in information handling, in accordance with the established policies and procedures. • To continuously improve the implementation, maintenance, and strengthening of established controls to protect information assets against new threats and changes occurring within the company, the environment, or in technologies.

- Comply with the legal requirements associated with information security, as well as the established good practices for the sector.

The other documents and policies that support the Information Security Management System will be stored in document management software for free consultation.

Communication

	Information security policy	Expiration date	
FYCO		Version	02
	Information security	Information classification	Internal use

This policy will be made available to employees, contractors, customers, suppliers and other interested parties and will be kept available on magnetic media in our information repository and published on the website for free consultation.

Policy review

This policy should be reviewed at least once a year or when significant changes occur, to ensure its suitability, adequacy and continual improvement.

_____

Edgar Juárez
CEO at FYCO

January 2024.