Corporate Policies

INFORMATION SECURITY POLICY

To all the Employees

All employees have a duty to protect the information of FENOCO. Therefore, this policy establishes the guidelines that must be followed to guarantee the security of the Company's information inside and outside of it.

As a member of the FENOCO team, the participation of each and every one id requested, in the protection of our information in compliance with the security policies of the information, standards and procedures presented in this document, and informing about any behavior that does not comply with our policy.

PRINCIPLES

The corporate principles that frame this policy are the following:

Respect
Operations performed under the strictest compliance with standards and procedures in an atmosphere of cordiality and solidarity with our stakeholders and the environment.

Integrity
Responsibility for results, acting with consistency and honesty in search of excellence..

Safety
Strengthening of timely risk analysis, generating a culture of self-care and assurance of our operation and the well-being of our people and communities.

Sense of Belonging
Characterized by our commitment, diligence and opportunity in decision making and meeting objectives.

1. OBJECTIVE

The objective of this policy is to establish the regulations and guidelines on the management of information security, aimed at mitigating the risks related to the treatment of the digital documents of the company.

2. SCOPE

The information security policies cover all the administrative and control aspects that must be fulfilled by any person with access to the information assets of FENOCO, in order to obtain an adequate level of security protection and the quality of the information of FENOCO

3. CONTENT OF THE POLICY

3.1. Statement of the Mission of Information Security.

"The protection of the information of FENOCO and the assets that constitute the Information systems, from failures that affect its availability, reliability, confidentiality, and integrity."

3.2. Functions and Responsibilities

Anyone with access to the information assets of FENOCO (employees, contractors, consultants, suppliers, business partners, or contractors of temporary employees of FENOCO) is responsible for the safe handling and protection of the company's information assets.

3.3. Principles of the Policy

3.3.1. Timely and accurate communication

Violations, problems, observed or suspected vulnerabilities, incidents or threats against the security of the information, must be reported through the channels established by the company in the Program of Attention of Concerns for the reception of these reports.

3.3.2. Compliance and conformity

All persons (employees, contractors, consultants, suppliers, business partners, or temporary employees) with access to FENOCO's assets and information temporarily or permanently are responsible for complying with the information security policy.

Anyone who tries and / or violates the security controls and mechanisms of the systems or networks would be subject to disciplinary actions in accordance with the provisions of the Internal Labor Code and / or Code of Conduct of the company.

3.4. Code of Information Security Practices.

3.4.1. Policies on the use of computers

FENOCO's communications systems, including the Internet, corporate messaging, and computer systems, are owned by the Company and must be used for its purposes.

3.4.2. Personal use of the Internet and Corporate Messaging

FENOCO recognizes that employees may use computer systems occasionally or require the use of the Internet or email for personal purposes. These communications will be considered private as long as the user files or catalogs them as personal.

3.4.3. Forbidden activities

The resources of FENOCO cannot be used for any of the following activities:

- Receive, view, share, or distribute materials that may be considered offensive or prohibited under Colombian law and Company policies.
- For commercial or personal ads.
- To solicit sales or promote outside business.
- Political pressure or publicity of political activities.
- Any commercial purpose other than the mission object of FENOCO.
- Distribute or share confidential or sensitive information of the company through instant messaging applications, free applications or non-corporate tools (Skype, WhatsApp, Line, and Messenger, among others).

Users of FENOCO networks are prohibited from using security test tools, network packet analyzers, "Sniffers", or similar tools and / or technologies. The authorization of these tools are only allowed for the Information Technology Department in the case they are required for diagnoses of failures and problems that occur in the network and which must be documented.

3.4.4. Privacy Waiver Policy

FENOCO users renounce all their privacy rights in relation to any element or corporate information that they create, store, send, or receive on FENOCO's computers or through FENOCO's Internet infrastructures.

The information cataloged and / or archived as personal by the users will be considered as private and confidential information of the users.

FENOCO reserves the right to supervise that computer and network systems are used in compliance with the Code of Conduct and the policies of FENOCO, which is expressly accepted by employees when signing the express consent of the right of Fenoco to verify compliance with them.

Fenoco may monitor the proper use of IT resources, including e-mail, internet use, file storage and access to computers. This supervision will allow Fenoco to record any misuse of the systems, as well as the creation, processing and storage of information contrary to Fenoco's policies, or that violate norms and laws.

3.4.5. Laptops

3.4.5.1. Physical Security of Laptops.

Laptops must be physically secured (maintained).

Users who are assigned laptop computers must assume all the safety responsibilities of the laptop and the information, programs, data stored in it. In addition, they must carry out the respective report of the loss to the corresponding state entities as soon as possible.

3.4.5.2. Backing Up Laptops

It is the responsibility of the IT Department that all the data stored in the laptops must be backed up at least biweekly in a centralized server or removable media (USB Drive, External Disks, etc.)

The IT Department is responsible for the security of all removable media where it makes its backups (USB Drive, External Disks, etc.).

3.5. Logical Access

3.5.1. Access to information

Users must have the approval of their immediate superior to access information systems or applications. Access to information must be granted to the individual based on the responsibilities of the user's position.

3.5.1.1. Password Protection

- Passwords are considered personal and non-transferable and must be well protected by each user.
- Passwords must not be written and left in a place where unauthorized persons can access them.
- Passwords must not be sent by email, except in correctly coded messages.
- The vulnerability of the passwords will be the responsibility of the owner of the same if he/she does not comply with what is described in the previous points.

3.5.2. Clean Desk Policy

Confidential documents or removable media containing confidential information must not be left where someone could pick it up easily, such as the copier, printer, fax machine, or an office or insecure workspace.

3.6. Virus Prevention

3.6.1. Anti-Virus Software

The Technology Direction will be responsible for installing and activating anti-virus software on each company's desktop, laptop, and server computer.

Each disk, USB drive or other means to transfer data to a computer must be examined by antivirus software before making use of the information contained therein.

3.6.2. Email

Attachments to incoming e-mails must be scanned for viruses on computers.
Users should not distribute chain mail through the company's messaging system

with information that is contrary to FENOCO's policies or that violate the rules and laws.

3.7. Copyright Policy

3.7.1. Software Registration

FENOCO's policy is to use Licensed Software. Therefore the computers are restricted for the installation of illegal software (Not registered). Users who attempt or violate these controls and install illegal software will be responsible for criminal sanctions and would be subject to disciplinary action in accordance with the provisions of the Company's Internal Labor Code and / or Code of Conduct.

3.7.2. “Shareware” and “Freeware”

It is forbidden to install shareware or freeware software in FENOCO's computer equipment.

3.8. Internet Connection Policy

3.8.1. Access to the Internet

The Technology Division must ensure that Internet access within FENOCO's infrastructure is carried out by means of a Firewall.

3.8.2. Web Browsing

Users are prohibited from downloading freeware and shareware programs.

3.8.3. Appropriate Web Sites

Access to inappropriate sites using FENOCO's equipment and technological infrastructure is prohibited. Examples of sites of this type could include, but are not limited to:

- Sexually explicit Web sites.
- Sites for *hackers*.
- Sites related to Warez (*illegal software* or tools for *hackers*).
- Sites that could conflict with the policies and / or commercial interests of FENOCO.

3.8.4. Prohibited Activities on the Internet

- Re-mailer services
- Users must not use the Internet for playing games.
- Users must not use their Internet access to send or download pornographic materials, inappropriate text files, or files that compromise the integrity of the network.

3.8.5. Remote Connections

All remote or external access to FENOCO networks and infrastructure must be done using VPN client connections through the Firewall; each user who uses or makes use of this type of connection must have a personal and non-transferable user and password and must be adequately guarded by each user.

4. GLOSSARY

- Vulnerability: Weaknesses that allow an attacker to compromise the integrity, availability or confidentiality of a computer system.
- Sniffers: A computer program that records the information sent by the peripherals.
- Anti-virus: A computer program intended to detect and remove viruses from computer systems.
- Shareware: Software distribution mode, in which the user can evaluate for free the product, but with limitations in the time of use or in some of the forms of use or with restrictions in the final capacities
- Freeware: Type of software that is distributed at no cost, available for use.
- Firewall: Computer program, hardware or combination of both that controls the access of a computer to the network and elements of the network to the computer, for security reasons.
- Hacker: Person who discovers the weaknesses of a computer, system or a computer network.

5. VALIDITY

This policy enters into effect as of October 18, 2017 and supersedes all previous provisions and will remain in force until a new policy modifies or supersedes the present.

ANDRÉS SOTO VELASCO
PRESIDENT