POLICY TITLE:	**INFORMATION SECURITY POLICY**
POLICY CODE:	PTI-04
ISSUANCE DATE:	May 2023
LAST REVISION DATE:	May 2023
REVISION Nº:	1
PREPARED BY:	Information Technologies
SCOPE:	All employees of the Organization, contractors, suppliers, and third parties.
OBJECTIVE:	This policy aims to establish the necessary rules and guidelines to ensure the security of the company's information, in order to protect the confidentiality, integrity, and availability of information in all its formats.

UNDER F.F.L:

Without legal fragment or provision.

GENERAL POLICIES AND GUIDELINES

a) Identify the necessary requirements and best practices to safeguard the security and integrity of Fibra Inn's information.

b) Ensure that all company personnel understand their duties and responsibilities when accessing company information, regardless of its format.

c) Prevent both accidental and intentional misuse of information, and reduce the impact of cybersecurity threats, unauthorized access, damage caused by negligence or lack of awareness, illegal activity, harassment, or fraud.

SCOPE AND GENERAL PROVISIONS

In accordance with the authorization granted to Fibra Inn collaborators to access and handle information generated within the organization, it is established that such access has a direct impact on Information Technologies, processes, and individuals. The following outlines the scope of this policy:

Scope of the Information Security Policy	
Information Technology	The IT team is responsible for ensuring operational continuity of the tools and/or platforms selected to support the organization's technological operations. This includes daily-use tools that store information at any level of the organization.
Processes	Processes are those implemented to ensure and safeguard the quality and integrity of information.
People	This policy applies to all active users within the organization who hold a valid employee identification number, as well as to suppliers and third parties under contract contributing to the company's goals

GENERAL PROVISIONS

- This policy sets forth the guidelines for:
  - Access to information
  - Information protection
  - Use of personal devices
  - Protection according to the level of confidentiality and type of information
  - Security incidents
  - Training and awareness

- The creation and handling of information must be conducted according to the confidentiality levels described in this policy.

- Information availability, whether on electronic devices or in physical format, must be treated with equal rigor, applying best practices to safeguard its integrity and confidentiality.

- Each user is responsible for decisions regarding information disclosure and must adhere to the organization's authorized guidelines.

- If, in the course of their duties, IT personnel detect any situation indicating potential information risk that may compromise the integrity and confidentiality of the information as established in this policy, they must report it to the Head of the IT Department and to either the Administration and Finance Department or General Management.

- The company is responsible for raising awareness and training all personnel to understand and properly fulfill their responsibilities in the protection of information as described in this policy. It is also the responsibility of each employee, contractor, or third party to comply with the regulations outlined herein.

- The IT Department is responsible for establishing device usage guidelines and regulations that safeguard the quality and confidentiality of information.

ACCESS TO INFORMATION IN DIGITAL MEDIA

- Access permissions must be established according to the employee's role and responsibilities.
- Users must authenticate before accessing information.
- Information access must be restricted to employees who require it to carry out their job functions.
- Policies regarding the separation of duties must be established to reduce the risk of fraud and error.

INFORMATION PROTECTION

- All mobile devices containing company information must be secured with strong access passwords (as established in the **GENERAL PASSWORD POLICY**) and data encryption.
- Physical documents containing confidential information must be stored in secure, locked locations.
- Electronic documents must be stored on secure servers with regular backups.
- Critical information must be regularly backed up to external storage devices and cloud environments.
- Policies on information retention and disposal must be implemented to ensure information is kept for the required period and securely destroyed when no longer needed.
- Access controls and surveillance systems must be implemented in data centers and other company facilities.

USE OF PERSONAL DEVICES

- Personal devices must not be used to access critical company information unless a formal agreement between the company and the employee has been previously established.
- Clear policies must be defined regarding the use of personal devices in the workplace.

- Personal devices used to access company information must have appropriate security measures in place.
- Clear policies must be established for remote data wiping in case of loss or theft of personal devices.
- Employees must immediately report any loss or theft of a personal device used to access company information.

PROTECTION ACCORDING TO INFORMATION CLASSIFICATION LEVEL AND TYPE

A classification model must be defined to identify and implement the necessary technical and organizational measures to ensure the availability, confidentiality, and integrity of the information. This classification model must align with the requirements and conditions established in this policy.

1. **Types of Information**
   a. **Logical media:** Information used through office software, email, or custom-developed or third-party information systems.
   b. **Physical media:** Information in printed format, or stored on magnetic media such as USB drives, CDs, DVDs, etc.

2. **Classification Levels**
   Depending on the sensitivity of the information, Fibra Inn will classify it under five levels. See the specific definitions in Annex A "**Information Classification Levels"**:
   a. Public Use
   b. Limited Distribution
   c. Confidential Information
   d. Restricted Information
   e. Secret Information

3. **Privileged Information Management**
   Information classified as restricted, confidential, or secret must be handled with special care. Extraordinary or additional security measures must be established to ensure the appropriate handling of privileged information. This type of information must be transmitted in encrypted form and through secure protocols.

4. **Information Privacy**
    - The organization and its collaborators must guarantee the privacy of personal data in order to protect the fundamental rights of individuals, particularly their right to honor, personal and family privacy, and personal image, through the establishment of measures to regulate the processing of such data.
    - The organization and its collaborators must comply with applicable personal data protection laws according to the jurisdiction in which they are established and operate. This includes compliance with the Mexican Data Protection Laws and the implementation of necessary measures to meet regulatory requirements.

SECURITY INCIDENTS

- Employees must immediately report any identified or notified security incident.
- The company must have an incident response plan that includes procedures for notification, assessment, containment, recovery, and improvement.
- A dedicated team must be established to manage security incidents.
- Security incidents must be documented and analyzed to determine root causes and define preventive measures.

TRAINING AND AWARENESS

- The organization must ensure that all personnel receive an adequate level of training and awareness in Information Security within the timelines required by current regulations, particularly in matters of confidentiality and information leakage prevention.
- Employees must also be informed of updates to security policies and procedures that affect them, as well as of existing threats, to ensure proper compliance with this Policy.
- Additionally, employees are required to act diligently regarding information management and ensure that such information does not fall into the hands of unauthorized employees or third parties.

CONSEQUENCES OF MISUSE

Failure to comply with or omission of the practices described in this policy may result in administrative, disciplinary, or legal actions as established by the organization.

ANNEX A. INFORMATION CLASSIFICATION LEVELS

CLASSIFICATION LEVELS:

Level	Level Detail	Examples
Public Use	Data that may be accessed by any individual. Malicious use of such information does not represent a threat to FINN's interests.	Any information available on Fibra Inn's official website.
Limited Distribution	Information used by different departments within FINN. If fraudulently used, it may pose a minor risk to the company's interests.	Any information such as emails and working documents.
Confidential Information	Confidential data accessible only to a select group. Fraudulent use could significantly impact FINN's interests.	Any audit report or organizational strategic planning document.
Restricted Information	Information intended exclusively for the owner. Disclosure could cause significant harm to FINN's interests.	Business communication or strategy between senior executives and shareholders involving operational continuity decisions.
Secret Information	Information that, if disclosed without authorization, may cause extremely serious damage to FINN's interests.	Information on acquisitions, divestitures, or any event that could affect the company's stock price in the securities market.

SIGNATURE SECTION

Authorized/Rewviewed by	Position	Signature
OSCAR E. CALVILLO AMAYA	Chief Executive Officer	
MIGUEL ALIAGA GARGOLLO	Chief Financial and Administrative Officer	
JUAN A. RIVAS CARRIÓN	Information Technology Director	