Cybersecurity Policy

Fibra Danhos

Administradora Fibra Danhos

INTRODUCTION

Fibra Danhos (FD) is a Mexican Real Estate Investment Trust (REIT) established primarily to develop, own, lease, operate and acquire iconic and premier quality real estate assets in Mexico.

Administradora Fibra Danhos (AFD) is a subsidiary company of Fibra Danhos (FD), which, through a Management Agreement, and in accordance with the instructions of the Trust Technical Committee, is empowered to carry out all the necessary or convenient acts for the fulfillment of the Trust's purposes, including the hiring of personnel and contractual relationships with suppliers and service providers.

AFD considers that the information and associated systems are critical assets that must be protected to ensure the proper functionality of the company.

The Cybersecurity Policy aims to effectively manage the security of the information processed by FD and AFD's computer systems, as well as the assets that participate in their processes.

The purpose of this Policy is to guarantee the confidentiality, integrity, availability and privacy of the information, and to comply with the Laws and Regulations in force at all times, maintaining a balance between risk levels and efficient use of resources, with criteria of proportionality.

This cybersecurity policy is applicable to all employees, directors and administrators of AFD, within the limits provided for in the applicable regulations.

BASIC PRINCIPLES

To achieve this, the following basic principles are established:

- Guarantee that the Information and Telecommunications Systems available to FD and AFD have the appropriate level of cybersecurity and resilience.
- Make all employees, contractors and partners aware of cybersecurity risks and ensure that they have the necessary knowledge, skills, experience and technological capabilities to support AFD's cybersecurity objectives.
- Strengthen prevention, detection, reaction, analysis, recovery, response, investigation and coordination capabilities against new threats.
- Promote the existence of appropriate cybersecurity and resilience mechanisms for systems and operations managed by third parties that provide services to FD and AFD.
- Establish procedures and tools that allow agile adaptation to the changing conditions of the technological environment and new threats.
- Collaborate with relevant government bodies and agencies to improve cybersecurity, comply with current legislation and contribute to improving cybersecurity in the international arena.

MANAGEMENT MODEL

AFD has a management model applicable to cybersecurity based on international and national regulations, to detect threats and obtain the necessary resources to meet the established cybersecurity objectives.

The model defined by AFD is based on:

- A framework for the management of the applicable measures through a risk methodology approved by the management in which the cybersecurity objectives and goals are set, as well as the principles aligned with the business strategy and consistent with the context where the activities of FD and AFD are carried out.

- Mechanisms to align cybersecurity goals and objectives in compliance with legislative, regulatory and contractual requirements.

- Mechanisms to react to incidents that occur both in the management of the system and in the operating procedures that depend on it.

- The existence of a set of functions and responsibilities regarding cybersecurity clearly defined and assigned in the corporate organization chart.

- Mechanisms for the global treatment of cybersecurity threats, including all appropriate activities for the treatment of security.

- A process of review and continuous updating of the cybersecurity management model to adapt it at all times to the cyber threats that arise and may affect FD and AFD.

Shared responsibility for cybersecurity:

FD and AFD employees and collaborators must comply with the best cybersecurity practices based on the following responsibilities:

- Detect suspicious actions or possible cybersecurity attacks in order to prevent and mitigate its possible negative impacts on the organization.

- Report suspicious actions or possible cybersecurity attacks on their work sessions (server session and/or mail client) to the IT area in a timely manner.

- Participate with the IT area, if necessary, during the process of investigation and resolution of the case.

FD and AFD are aware that in order to reduce cybersecurity risks, the guidelines in this policy must become a common practice among their employees and collaborators. Anyone related to FD and AFD can report a cybersecurity risk via email tecnologias@danhos.com.mx or by phone (55) 5284-0030 ext. 8001 and 8003, generating an invoice for follow-up.