



Cybersecurity Policy

Fibra Danhos

Administradora Fibra Danhos



INTRODUCTION

Fibra Danhos (FD) is a Mexican Trust established mainly to develop, own, lease, operate, and acquire iconic and premier quality commercial real estate assets, offices, mixed-use projects, industrial warehouses, and projects in the tourism sector in Mexico.

Administradora Fibra Danhos (AFD) is a subsidiary company of Fibra Danhos (FD), which, through a Management Agreement, and under the instructions of the Trust Technical Committee, is authorized 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.

SCOPE

Guarantee the confidentiality, integrity, availability, and information privacy. Comply with current laws and regulations all the time. Keep a balance between risk levels and efficient resource use.

REACH

AFD considers information and systems as critical assets that need to be protected to ensure the correct functioning of the company, which is why the Cybersecurity Policy applies to all employees within the limits provided for in the applicable regulations.

COMMITMENTS

- Guarantee that the Information and Telecommunications Systems available at FD and AFD have the appropriate cybersecurity and resilience levels.
- Raise awareness among all employees, contractors, and employees about cybersecurity risks and ensure they have the knowledge, skills, experience, and technological capabilities necessary to support AFD's cybersecurity targets.
- Strengthen prevention, detection, reaction, analysis, recovery, response, investigation, and coordination capabilities against new threats.
- Promote the existence of adequate cybersecurity and resilience mechanisms for systems and operations managed by third parties that provide services to FD and AFD.
- Define procedures and tools that allow you to adapt quickly to the changing conditions of the technological environment and new threats.
- Collaborate with relevant government organizations and agencies to improve cybersecurity, comply with current legislation, and contribute to the improvement of cybersecurity internationally



MANAGEMENT MODEL

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

The defined model for AFD involves the following;

- A framework for managing applicable measures through a risk management methodology, with cybersecurity objectives and principles aligned with the business strategy and consistent with the national context.
- Mechanisms to align cybersecurity targets and goals in compliance with legislative, regulatory, and contractual requirements.
- Incident reaction mechanisms in system management and operational procedures that depend on it.
- A set of defined functions and responsibilities regarding cybersecurity duly assigned in the corporate organizational chart.
- Cybersecurity threats global mechanisms, including all appropriate activities for security treatment.
- A continuous review and updating of the cybersecurity management model to adapt to any cyber threats that arise and may affect FD and AFD.

GRIEVANCE MECHANISMS

AFD asks all its stakeholders to report any concerns or feedback they have regarding cybersecurity risks in our operations or value chain through its ethics line. This same channel is available so that breaches that are detected can be reported anonymously.

You can make your complaint through the portal <https://danhosteescucha.lineaetica.com.mx> or email danhosteescucha@lineaetica.com.mx, generating a folio for monitoring.

POLICY REVIEW

AFD undertakes to review this policy annually with the possibility of modifying and updating it at any time. Changes to this policy will come into effect immediately once it is updated on the website, so we encourage the reader to review this policy regularly.

RELATED POLICIES

- Code of Ethics
- Suppliers Code of Conduct
- Stakeholders Relations Policy



DOCUMENT CONTROL

Version	Approved by	Date of last review/update
1.0	Blanca Canela, Executive Director of Administradora Fibra Danhos	November, 2022
2.0	Blanca Canela, Executive Director of Administradora Fibra Danhos	December 2023