POLICY TITLE:	**CYBERSECURITY INCIDENT AND ATTACK RESPONSE POLICY**
POLICY CODE:	PTI-06
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 clear and effective procedures to identify, respond to, and mitigate cybersecurity incidents, thereby minimizing their negative impact on the organization. It also seeks to ensure business continuity and protect the confidentiality, integrity, and availability of data.

UNDER F.F.L:

Without legal fragment or provision.

GENERAL POLICIES AND GUIDELINES

a) Establish a general guideline for responding to potential cyberattack situations.

b) Ensure that all company personnel understand their duties and responsibilities when targeted by potential cyberattacks.

c) Prevent the accidental or intentional misuse of information and mitigate the impact of cybersecurity threats.

SCOPE AND GENERAL PROVISION

As part of the authorization granted to Fibra Inn employees who interact with the organization’s systems, data, and resources, it is determined that this has a direct impact on Information Technology, processes, and people. The scope of this policy is outlined below:

Scope of the Information Security Policy	
Information Technology	The Information Technology team is responsible for managing the operational continuity of the tools and/or platforms selected to support the organization’s technological operations. This includes the daily-use tools that host information at any level within the organization. Additionally, the IT team is responsible for providing ongoing training to ensure the continuous updating of knowledge regarding risk factors that may affect the organization.
Processes	Processes refer to those implemented to ensure timely response in the event of a potential technological attack.
People	This policy applies to all active users within the organization who have a valid employee ID number, as well as to providers and third parties who have a contract that links them to the achievement of the company’s objectives.

GENERAL PROVISION

This cybersecurity policy provides a solid framework to effectively address cyber incidents and attacks while protecting the organization’s assets. It is essential to adapt it to the specific needs of your organization, involving cybersecurity experts to ensure its effectiveness and relevance.

RESPONSIBILITIES

Incident Response Team (IT Support)

- Appoint a leader for the incident response team. See Annex A **“Cyberattack Scalation Matrix”.**
- Identify, analyze, contain, mitigate, and recover from cybersecurity incidents. See Annex B **“Technology Responsibility Matrix by Incident Level”.**
- Coordinate and collaborate with relevant teams to ensure an efficient and effective response.
- Keep updated documentation of incidents, actions taken, and lessons learned.
- Conduct regular incident response drills and testing.

IT and Security Team

- Provide technical support to investigate security incidents and carry out response actions.
- Collaborate in the implementation of preventive and corrective measures based on lessons learned.
- Maintain an up-to-date inventory of assets and their security status.

Organization Personnel

- Immediately report any suspected or actual security incident through the designated channels.
- Collaborate with the IT support team in incident investigation and response.
- Participate in cybersecurity training and awareness programs.

INCIDENT RESPONSE PROCEDURES

Detection and Identification of Incidents

- Establish alert systems and monitoring tools to detect potential security incidents.
- Promote a culture of incident reporting to ensure early detection.
- Investigate and assess the nature and scope of the incident to determine its severity and classification.

Incident Classification and Prioritization

- Classify incidents based on their severity, impact, and risk level to the business. See Annex C **“Cyber Risk Matrix”.**
- Use a scoring system or risk matrix to prioritize response actions.
- Establish a review group to validate the classification and prioritization of incidents.

Containment and Mitigation

- Conduct a forensic analysis to determine the root cause of the incident and the vulnerabilities exploited.
- Implement temporary fixes and security patches if necessary, following a controlled change management process.
- Establish clear communication lines and authorization channels for containment actions.

Investigation and Forensic Analysis

- Conduct a forensic analysis to determine the root cause of the incident and the vulnerabilities exploited.
- Document all evidence securely and confidentially for potential legal or investigative actions.

Notification and Communication

- Notify relevant internal and external stakeholders about the incident and the actions taken.
  - ○ Provide periodic monthly reports to the Administration and Finance Department and/or General Management on all events reported as potential cybersecurity threats and risks that may affect Fibra Inn.

- Coordinate communication with regulatory and legal authorities in accordance with applicable laws and regulations.
- Prepare communication templates to ensure swift and accurate responses.

Recovery and Continuous Improvement

- Restore affected systems and data to a secure and functional state.
- Analyze the incident to identify lessons learned and improvement recommendations.
- Update policies, procedures, and security measures accordingly.
- Conduct post-incident review meetings to discuss necessary improvements and adjustments.

TRAINING AND AWARENESS

Conduct periodic cybersecurity training, including incident response drills, for all employees. Regular awareness programs must also be implemented to foster a strong security culture across the organization.

REVIEW AND UPDATE

Review and update this policy and its procedures on a regular basis to ensure alignment with cybersecurity best practices and evolving technological and operational environments. Conduct internal and external audits to assess compliance with the policy.

CONSEQUENCES OF MISUSE

Failure to comply with or omission of the practices described in this policy will result in administrative, disciplinary, or legal measures as determined by the organization.

APPENDIX A. CYBERATTACK ESCALATION MATRIX

This matrix defines the scale of cyberattacks based on scope, complexity, and the company departments to be notified immediately.

Attack Scale	Description	Examples	Immediate Notification
Low Scale	Isolated or low-impact attacks affecting specific individuals or systems.	Phishing attack targeting a single employee.	1.- Technical Support 2.- IT Department
Medium Scale	Attacks targeting a broader group of users or systems, yet manageable with standard security actions.	Ransomware attack affecting a department or a branch.	1.- IT Department 2.- Technical Support 3.- Direction of Administration and Finance 4.- General Management
High Scale	Large-scale attacks that may compromise multiple systems and networks, affecting the entire organization.	DDoS attack against the company's infrastructure.	1.- IT Department 2. Technical Support 3. General Management 4. Direction of Administration and Finance
Very High Scale	Highly coordinated and sophisticated attacks targeting multiple organizations at national or global level.	Attack by a state-sponsored hacking group impacting multiple organizations across countries.	1.- IT Department 2. Technical Support 3. General Management 4. Direction of Administration and Finance

APPENDIX B. TECHNOLOGICAL RESPONSIBILITY MATRIX ACCORDING TO INCIDENT SCALE

This matrix provides a structure to understand how the IT Support Team's response varies depending on the severity and scope of the incident. Each escalation level implies an increase in the complexity of actions and the need for coordination with various internal and external stakeholders.

Incident Scale	Description	Actions by the IT Support Team
Low Scale	Isolated or low-severity incidents that can be handled internally with established procedures.	- Investigation and analysis of the incident. - Immediate containment and mitigation. - Documentation and lessons learned for continuous improvement.
Medium Scale	Incidents requiring broader coordination and response involving multiple departments or systems.	- Coordination with relevant departments. - Detailed forensic analysis. - Expanded containment and mitigation actions. - Internal notification and communication.
High Scale	Severe incidents impacting a wide part of the organization, requiring urgent and coordinated response.	- Immediate action following a detailed incident response plan. - Interdepartmental coordination and involvement of external experts. - Coordinated communication with authorities.
Very High Scale	Massive incidents affecting the entire organization or even national/global levels, requiring large-scale coordination and potentially support from external organizations or governments.	- Comprehensive and agile coordination with all relevant departments and teams. - Active collaboration with government agencies, industry experts, and cybersecurity bodies. - Mobilization of additional resources as needed.

APPENDIX C. CYBER RISK MATRIX

This risk matrix evaluates each type of cyberattack based on its **probability** and potential impact. The **Risk Level** is derived by combining the **probability** and **Impact**, offering a clear view of the threat severity to the organization.

Type of Attack	**Probability** (High, Medium, Low)	**Impact** (High, Medium, Low)	**Risk Level** (High, Medium, Low)
Phishing	High	High	High
Malware	Medium	High	High
DDoS Attack	Medium	High	High
SQL Injection	Medium	High	High
Brute Force Attack	Medium	Medium	Medium
Social Engineering Attack	High	Medium	High
Web Attack	Medium	Medium	Medium
Network Attack	Medium	Medium	Medium
Zero-day Attack	Low	High	Medium
Ransomware	Medium	High	High

SIGNATURE SECTION

Authorized/Reviewed 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	