Ferreycorp	**CYBERSECURITY AND INFORMATION SECURITY CORPORATE POLICY**	**CÓDE**	**VERSIÓN**
		GEN-GTPI-PC-001	02
		INITIAL EFFECTIVE DATE	**FINAL EFFECTIVE DATE**
		03.01.2023	**04.01.2028**
PROCESSING MANAGEMENT	CORPORATE IT MANAGEMENT PROCESSES AND INFORMATION		
ELABORATED BY	**REVIEWED BY**	**APPROVED BY**	
Eduardo Luyo Vicente	Eduardo Tirado Hinojosa	Mariela García Figari De Fabbri	
INFORMATION SECURITY OFFICER	CORPORATE MANAGER IT PROCESSES AND INFORMATION	GENERAL MANAGER	

1. Objective:

The objectives of this policy are to protect the data, systems and information technologies of the companies and entities of Ferreycorp Corporation.

2. Scope:

This policy applies to all employees and third parties with access to the data, systems and information technology of any of the Corporation's companies.

3. Definitions:

The following terms are defined below:

3.1 *Cyber-attack.* - is a type of malicious activity carried out by cybercriminals that attempts to collect, disrupt, deny, degrade or destroy information systems or the information itself.

3.2 *Cybersecurity.* - is the process of protecting information systems and information itself from cyber-attacks.

4. Content

Cybersecurity:

4.1. At Ferreycorp Corporation, the use of new technologies and applications including mobility, use of cloud services, use of applications as a service, remote access to our network, integration with third-party systems, use of artificial intelligence, robots and others must consider risk assessments, definition and implementation of controls against cyber-attacks and cybersecurity tests.

4.2. All technologies in use, as well as networks and cloud services, should have regular vulnerability scanning and ethical hacking reviews in order to detect and remediate any security breaches in them.

4.3. Technologies that do not comply with cybersecurity controls should not be used in any business operation because they could expose the Corporation's technology infrastructure, applications or data.

4.4. TPI's Corporate Management shall establish the mechanisms for prevention, detection and recovery.

(i) Prevention: deploy early monitoring mechanisms and protocols to ensure that all information and supporting technologies are protected against cyber threats.

(ii) Detection: having the capabilities to respond to a cyber-attack.

(iii) Recovery: implement and implement recovery plans to reduce the impact of a cyberattack, cyberattack monitoring and detection systems, as well as response and/or recovery procedures for the Corporation's technological infrastructure, applications, and data.

4.5. All managers and collaborators who identify any malicious event such as spam, phishing, malware in their computer equipment, networks, mail or applications, must immediately report it to the Information Security Area for the adoption of containment and remediation measures.

Information Security

4.6. For Ferreycorp Corporation, data from its business operations, customers, employees, suppliers and shareholders should be considered an intangible asset.

4.7. Given the importance, high value and usefulness of the data, the companies and entities of the Ferreycorp Corporation have the duty to preserve and take care of it, based on the following principles:

- Compliance with required legislation and regulations
- Access management based on the "need to know" for strict business reasons and according to the employee's role in each area.
- Commitment of the collaborators in the handling of information in accordance with the role they play.
- Data must be protected according to its value and importance.

4.8. Information security practices will protect the value of business information assets and will be aligned with international best practices and standards.

4.9. All employees working in the companies and entities of Ferreycorp Corporation are responsible and committed to protect the resources and information they handle, as well as to comply with and enforce the information security regulations

4.10. Ferreycorp Corporation is committed to the lawful use, treatment in accordance with the established purposes and protection of personal data that collects, stores, uses, circulates or deletes in accordance with the protection laws in each country where we operate.

4.11. Any information and intellectual property (software, trademarks, databases, designs, manuals, images, etc.) belonging to any of the Corporation's companies must not be used for private purposes or transferred to third parties.

4.12. It is the responsibility of all Managers and Collaborators to report to the Information Security Officer the events and incidents of information security occurred in order to establish corrective actions.

4.13. Any breach of an information security policy, rule, standard or procedure by any employee shall be considered a cause for disciplinary action. If the non-compliance originates from any contractor, the company may suspend the provision of the service.

THIS DOCUMENT HAS BEEN AUTHORIZED IN THE REGULATORY SYSTEM BY:

ROLE	NAME	POSITION	DATE
Developer	Eduardo Luyo Vicente	INFORMATION SECURITY OFFICER	Approved - 04/03/2023 14:10
Reviewer	Eduardo Tirado Hinojosa	CORPORATE MANAGER IT PROCESSES AND INFORMATION	Approved - 04/10/2023 08:36
Approver	Mariela García Figari De Fabbri	GENERAL MANAGER	Approved - 04/12/2023 15:20