PicPay	**Responsible area:** Cybersecurity
Police	**Classification:** External
	Site: 01
CYBERSECURITY	

Summary

The information contained in this document must be used exclusively for **EXTERNAL** use

1. Objective

This Cyber Security Policy (“Policy”) aims to establish guidelines and guide Employees, Partners, Customers and Service Providers on the rules to ensure the application of controls and administrative measures necessary to protect Information owned or held by companies. entities PicPay Institution of Payment S.A., PicPay Bank- Banco Múltiplo S.A., PicPay Invest DTVM S.A, Cred novo SEP S.A and all their respective entities subsidiaries (directly or indirectly controlled entities), hereinafter referred to as (“PicPay Group”), for the purpose of complying with the main regulations in force of Branco Central do Brasil and other competent bodies.

2. Approval Forum

This Policy is approved by the Board Committee.

3. Validity

This Policy will be valid for 1 (one) year, or, in a shorter period, when the responsible forum that approved deem necessary, starting from the date of approval by the Board of Directors.

4. Application and Target Audience

This Policy applies, in Brazil and abroad, to PicPay Group companies as well as to all its administrators and employees, including any interaction with customers, partners, suppliers and other stakeholders.

5. Definitions and Abbreviations

For a better understanding of this Policy, we have listed in alphabetical order the main concepts referred to in this document, in order to avoid difficulties in interpretation or ambiguities:

Information Asset: Any resource capable of processing, storing or transmitting information.

Threat: Potential cause of an unwanted incident, which could result in damage to the company's systems or information.

Backup: The process of copying data from one storage device to another to provide protection against the loss of the originals.

Access Control: They are logical or physical barriers that prevent or limit access to information, as well as protecting it from unauthorized modifications.

The information contained in this document must be used exclusively for **EXTERNAL** use

Workforce: Name given to the person hired whose employment relationship is governed by the CLT - Consolidation of Labor Laws in Brazil.

Cryptography: Techniques used to transform information from its original form to an unreadable one, so that it can only be known by its recipient (holder of the “secret key”), which makes it difficult to be read by anyone unauthorized.

Information Classification: Process that aims to identify and define appropriate levels and criteria for the protection of information, according to its importance for organizations.

Source code: A set of text files containing all the instructions that must be executed by the computer logically in a programming language.

6. Guidelines

The Cybersecurity Policy establishes the guidelines that guide the implementation of controls, processes and procedures aimed at cybersecurity in the PicPay Group, following the following principles:

I. **Confidentiality:** guarantee that all Information will only be accessible to authorized people, guaranteeing the concept of “least possible privilege”.

II. **Integrity:** guarantee that the information, whether stored or in transit, is complete, accurate and will not undergo any unauthorized modification or deletion.

III. **Availability:** guarantee that the Information will always be available when necessary; and

IV. **Authenticity**: guarantee of the veracity of the information, certifying that the Information is true and that has not changed in its life cycle.

6.1 Cyber Risk Management

The PicPay Group adopts processes to identify, assess, correct and monitor cyber risks. We analyze the criticality and impact of each cyber risk, adopting mitigation actions and periodic review to ensure compliance with best security practices.

6.2 Asset Management and Information Processing

The information contained in this document must be used exclusively for **EXTERNAL** use

PicPay Group information is classified and protected within Information Assets according to its sensitivity and importance to the business.

6.3 Security Posture

The security posture is based on prevention and readiness to respond to cyber risks, continuous monitoring of threats, the application of good security practices and the search for continuous improvement of security processes.

6.4 Logical Access Control

Logical access controls are implemented with the aim of controlling access to sensitive information, therefore applying the principle of least privilege, with periodic reviews of authorizations where it is possible to ensure the adequacy of access.

6.5 Physical Access Control

We maintain physical access control to PicPay Group facilities through registration and authorization, in addition to unique identification through badges and the use of biometrics, when necessary.

6.6 Monitoring, Control and Auditing

The PicPay Group uses mechanisms to guarantee the traceability of information. This continuous monitoring of actions in the technological environment allows us to identify and correct possible errors, guaranteeing traceability and data protection.

6.7 Threat and Incident Management

The PicPay Group has processes and mechanisms that continuously monitor threats in our Information Assets, ensuring the identification and elimination that may result in the compromise of our information.

6.8 Security in Operations

The PicPay Group develops mechanisms that guarantee that our products and services offered to our users are always available and protected from failures or unavailability using robust encryption protocols and periodic vulnerability reviews.

The information contained in this document must be used exclusively for **EXTERNAL** use

6.9 Business Continuity

The PicPay Group has business continuity strategies for critical processes, which are regularly evaluated and tested to ensure that services remain active in crisis situations.

6.10 Management of Suppliers, Service Providers and Partners

The PicPay Group has processes and methodology that guarantee the evaluation of its suppliers, partners and service providers in order to identify possible cyber risks that could compromise information security principles.

6.11 Networks and Communications

The PicPay Group adopts appropriate network and communication protection measures to ensure safe access for employees and authorized third parties.

6.12 Secure Development and Adoption of New Technologies

The PicPay Group adopts secure development practices during the development lifecycle of its products and services. Controls capable of identifying and correcting vulnerabilities are practiced in every technological environment.

6.13 Security Compliance Management

The PicPay Group implements robust processes and procedures to identify potential deviations from compliance with information security requirements, complying with applicable regulations and aligned with best market practices.

6.14 Culture and Awareness

The PicPay Group continuously establishes training on information security for employees and service providers, reinforcing the importance of security and promoting good practices through regular awareness campaigns.

6.15 Regulatory Demands

The PicPay Group is committed to complying with local and international regulations, including Law 13,709/2018, which deals with the protection of personal data of all natural persons who are part of

The information contained in this document must be used exclusively for **EXTERNAL** use

this ecosystem, in addition to carrying out periodic assessments to ensure compliance and maintain records documented for regulatory review.

6.16 Violation of Cyber Policy and Sanctions

The PicPay Group understands that violating the guidelines of this Policy constitutes a serious offense, subjecting those responsible to appropriate administrative and judicial measures. Security incidents or misconduct are recorded and evaluated, which may result in sanctions after analysis by the Compliance and Legal area.

7. Associated Internal Regulations

This Policy was developed based on the main Cybersecurity Frameworks, in order to meet the Security guidelines established by the Central Bank of Brazil and others regulatory bodies.

a) BCB Resolution no. 85/2021;
b) CMN Resolution No. 4,893/2021;
c) LGPD - General Data Protection Law 13,709/2018;
d) CVM - Securities and Exchange Commission Instruction No. 35/2021;
e) NIST - National Institute of Standards and Technology;
f) ISO/IEC 27001:2022 and ISO/IEC 27002:2022;
g) PCI DSS - Payment Card Industry – Data Security Standard;
h) ISO/IEC 27005:2023.

8. Attachments

N/A

10. Change History

Topic changed	Detailing	Date of change
N/A	Criação do Documento	04/11/2024

The information contained in this document must be used exclusively for **EXTERNAL** use