INFORMATION ABOUT BANCO RABOBANK'S CYBER SECURITY POLICY

1. INTRODUCTION

This document consists of a simplified version of the Cyber Security Policy of Banco Rabobank International Brasil S.A., hereinafter Banco Rabobank, and aims to demonstrate, in general terms, the controls adopted by Banco Rabobank to prevent, detect and reduce vulnerability in cyber environment related incidents.

The main objectives of this Policy are: (i) to guarantee the confidentiality, integrity and availability of information from Banco Rabobank's customers, employees and suppliers (ii) to adequately protect the Bank's systems and information, (iii) to guarantee the continuity of the Bank's business, protecting critical processes from interruptions, and (iv) to ensure that the purposes approved by the Bank are respected during the provision of third-party services when contracting data processing and/or storage services.

In this context, Banco Rabobank has information security governance, including policies, controls and risk management processes that ensure the reliability of its systems and the continuity of services relevant to the provision of banking services. The aforementioned security policies, controls and processes are in line with the best practices and international market standards and also seek to ensure the Bank's compliance with the laws and regulations applicable to information security, privacy and data protection.

Aiming at the continuous improvement of cybersecurity processes, the senior management of Banco Rabobank is committed to its Cybersecurity Policy and to the continuous improvement of cybersecurity processes, having designated a director responsible for the policy and for the execution of the action plan and cyber incident response.

2. SCOPE OF CYBER SECURITY POLICY

Banco Rabobank's Cyber Security Policy, which is periodically reviewed, covers the confidentiality, integrity and availability of information, as well as promoting the implementation of preventive, detective and corrective measures, aimed at controlling the cyber environment, mitigating potential incidents of cyber security and reduction of vulnerabilities related to the activities of Banco Rabobank.

3. TERMINOLOGY

For Banco Rabobank's Cyber Security Policy, the terms below have the following definitions:

- Cybersecurity: set of practices, policies, security concepts, risk management approaches, training and technologies used to protect the cyber environment, the organization, business continuity and the data of customers, employees, suppliers or business partners from Banco Rabobank.

- Cyber Incident: A security incident can be defined as any security-related event (occurrence or attempt) or any security breach related to security policies that has or may have:
    - Damaged property or caused damage to Rabobank employees or customers, or;
    - Affected the entity's ability to deliver appropriate services to customers; or;
    - Result in theft or fraud.

- Vulnerabilities: any conditions that, when exploited by an unknown person or person not linked to Rabobank (but could be a malicious contributor as well), could result in security breaches, such as failures in the design,

implementation or configuration of programs, services or network equipment, outdated or missing cybersecurity mechanisms. A vulnerability exploit attack occurs when an attacker attempts to perform malicious actions, such as breaking into a system, accessing confidential information, launching attacks against other computers, or rendering an application or service unavailable.

4. INFORMATION SECURITY MONITORING AND PREVENTION AGAINST CYBER ATTACKS

Banco Rabobank's information security monitoring and cyber-attack prevention process consists of identifying threats and vulnerabilities, defining security controls necessary to protect the business, testing and monitoring internal and external environments. The main objective is to prevent the realization of cyber threats.

5. APPLICATION SECURITY MANAGEMENT AND ADOPTION OF NEW TECHNOLOGIES

The main assumptions applicable to the adoption of new technologies by Rabobank include:

- The development of new applications must be in line with Rabobank's best security practices and guidelines related to secure development;
- The adoption of new technologies must also be subject to security controls proportional to the criticality classification of the asset, which go through classification processes, risk assessment and implementation of corrections or adjustments before and after being made available in the production environment;
- The implementation of information traceability controls and mechanisms;
- Security testing, such as penetration testing and secure code testing, must also be performed for the relevant services prior to implementation in the production environment;
- Conducting general security tests (such as compliance with security parameters); and,
- The implementation of controls that ensure the segregation between development, test and production environments, in order to reduce the risk of unauthorized access or undue changes in the operating environment, database and/or applications.

6. ACCESS CONTROL MANAGEMENT

The levels of controls applied in the management of access control of logical resources of Banco Rabobank vary according to the assessment of the risks associated with information and assets.

7. INFRASTRUCTURE MANAGEMENT / BUSINESS CONTINUITY

The controls adopted by Banco Rabobank in the development of infrastructure have as their primary objective to ensure that Banco Rabobank remains operational in the face of cyber threats, in order to ensure the confidentiality, integrity and availability of information, thus ensuring business continuity through scenario analysis, monitoring and testing for continuous improvement are part of this process.

8. CYBER INCIDENT RESPONSE PLAN AND MANAGEMENT

The management and response plan to cyber incidents for relevant services of Banco Rabobank are carried out considering the analysis of the cause, impact and effect of the incidents, as well as the identification and constant monitoring of risk scenarios and situations.

9. MANAGEMENT OF RELEVANT SERVICE PROVIDERS COMPANIES

Banco Rabobank adopts procedures for contracting data processing and storage and cloud computing service providers compatible with the provisions of Resolution no. 4,893/2021 of the National Monetary Council.

In managing its suppliers, Banco Rabobank mainly seeks to ensure the implementation of controls to prevent incidents to be adopted by suppliers that handle sensitive data or that are relevant to Rabobank's activities. Said controls must be compatible with the cybersecurity processes and mechanisms adopted by Banco Rabobank itself.

10. CONTACT

If you have any questions about this document or about the Cybersecurity Policy of Banco Rabobank, please contact the Rabobank division in which you do business, through our institutional website. (http://www.rabobank.com.br/en/contact/index.html) or via e-mail csirt.sa@rabobank.com.

11. LEGAL NOTICE