INFORMATION ABOUT THE CYBER-SECURITY POLICY OF RABOBANK BANK

1. INTRODUCTION

This document consist of simplified version on the Cyber Security policy of Banco Rabobank International of Brazil, hereinafter referred to as Banco Rabobank, and aims to demonstrate, in general terms, controls adopted by Banco Rabobank to prevent, detect and reduce vulnerability and incidents related to the cyber environment.

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

The Bank has security governance, including risk management policies, controls and processes that ensure the relevant services and applications for the provision of banking services, that ensure the reliability of its systems and the continuity of the relevant services for the provision of bank services. Such security policies, controls and processes are in line with the best international market practices and standards and aim to ensure the compliance of the Bank with the laws and regulations applicable to information security, privacy and data protection.

The senior management of Rabobank Bank is committed to its Cyber Security policy of and to the continuous improvement of cyber security processes, having appointed a director responsible for this policy and for the execution of the action plan for response to cyber incidents.

2. TERMINOLOGY

For the purposes of this document and the Bank's Cyber Security Policy, the terms below have the following definitions:

Cyber Security: set of practices, policies, safety concepts, risk management approaches, training and technologies used to protect the cybernetic environment, the organization, the business continuance and the data of Rabobank's customers, employees, suppliers or business partners.

- Cyber Security Incidents: any security incident that may occur within the Rabobank bank infrastructure and/or in the third-party service providers, which may result in violation of any privacy and information security, in the interruption of processes critical to the activities of the Banco Rabobank or, even in unauthorized access to data from Banco Rabobank, its customers, employees, suppliers or business partners. Incidents of outage or otherwise, which were not the result of exploiting a cyber-threat, such as a cyber-attack, are not considered as cyber incidents.

- Vulnerabilities: any conditions that, when explored by a malicious third party, could result in security violation, such as failures in the project, in the implementation or configuration of programs, services or network equipment, outdated or lack of cyber security mechanisms. An attack that exploit vulnerabilities occurs when a third attacker attempts to perform malicious actions, such as hacking into a system, accessing sensitive information, shooting attacks against other computers, or marking an application or service unavailable.

3. CYBER SECURITY POLICY SCOPE

Rabobank Cyber Security Policy, which is reviewed periodically, includes the guideline to ensure the confidentiality, integrity and availability of information, as well as preventive, detective/traceable, corrective measures, aimed at controlling the cyber environment, mitigating potential cyber security incidents and reducing vulnerability points.

4. MONITORING INFORMATION SECURITY AND PREVENTING CYBER ATTACKS:

The monitoring process for information security and the prevention against cyber-attacks against Rabobank Bank consist of identify threats and vulnerabilities, define the security controls necessary to the business protection, testing and monitoring of internal and external environments. The main objective is to avoid the occurrence of cyber threats.

5. APPLICATION SECURITY MANAGEMENT AND ADOPTION OF NEW TECHNOLOGIES

The main assumptions related with the application security management and adoption of new technologies by Rabobank include:

- The development of new, relevant service applications must be in line with the best security practices recommended by international standards and Rabobank Bank policies, specific to secure development;
- The adoption of new technologies must also be subject to security controls in proportion with the classification of criticality of the asset, so that such adoption undergoes through processes of classification, risk assessment and implementation of corrections or adjustments before and after being made available in the productive environment ;
- The implementation of Controls and traceability mechanisms;
- o The execution of Security testing, such as penetration testing and secure code testing must also be performed for relevant services prior to implementation in the production environment;
- o The execution of General security tests (such as safety parameters);
- o The implementation of controls to ensure segregation between development, testing and production environments, with the aim of reducing the risks of unauthorized access or improper changes in the operating environment, database and / or applications.

6. ACCESS CONTROL MANAGEMENT

The levels of control relied upon in the access control management of logical resources of Rabobank Bank vary according to the classification of the asset

7. INFRASTRUCTURE / BUSINESS CONTINUITY MANAGEMENT

The primary objective of Rabobank Bank controls in infrastructure development is to ensure that Rabobank Bank remains operational in the face of cyber threats in order to ensure the confidentiality, integrity and availability of information

therefore, ensuring business continuity through scenario analysis, monitoring and tests for continuous improvement are part of this process.

8. MANAGEMENT AND PLAN OF CYBERNETIC INCIDENTS RESPONSE

The management and plan of responses to cyber incidents for relevant services of Rabobank Bank must be performed considering the assessment of cause, impact and effect incidents, as well as the constant identification and monitoring of risk scenarios and situations. ,

9. MANAGEMENT OF THIRD PARTY RELEVANT SERVICE PROVIDERS

Banco Rabobank adopts procedures for retaining suppliers of data processing and storage services and cloud computing services in compliance with the provisions of Resolution 4,658 / 2018 of the Central Bank of Brazil.

In the management of its suppliers, Rabobank Bank primarily aims to ensure the execution of controls to prevent incidents to be adopted by suppliers that handle sensitive data or that are relevant to Rabobank Bank activities. Such controls must be compatible with the processes and cyber security mechanisms adopted by Rabobank Bank.

10.CONTACT

If you have any questions regarding this document or the Cyber Security Policy of Rabobank Bank, please contact the Rabobank division with which you have businesses, through our institutional website (http://www.rabobank.com.br/en/contact/index.html) or through this e-mail csirt.sa@rabobank.com.

11.LEGAL NOTICE