INFORMATION ABOUT THE CYBER-SECURITY POLICY OF BANCO RABOBANK

1. INTRODUCTION

This document consist of streamlined 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 to 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.

Therefore, Banco Rabobank has an apparatus for governance of information security, including policies, controls and risk management processes 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 Banco Rabobank 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 Banco Rabobank's customers, employees, suppliers or business partners.

- Cyber Incidents: any security or technical incidents that may occur within the technical environment of Banco Rabobank or third-party service providers, which may result in violation of any privacy and information security policies of Banco Rabobank, 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.

- 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

Banco Rabobank's Cyber Security policy, which is reviewed annually, includes controls 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. Among the main controls adopted by the Banco Rabobank are:

- Authentication;
- Cryptography;
- Invasion, prevention and detection;
- Prevention of information leakage;
- Periodic testing and scans for vulnerability detection;
- Protection against malicious software;
- Establishment of information traceability mechanisms; Access controls and segmentation of the computer network;
- Maintenance of backup copies of data and information;
- Secure Software Development;
- Implementation of new technologies;
- Incident management;
- Awareness of users, customers and suppliers:
    - Cybersecurity culture awareness initiatives, including the implementation of training programs and periodic assessment of employee awareness;
    - Cyber security awareness initiatives for customers, third-party companies and relevant service providers.

4. MONITORING INFORMATION SECURITY AND PREVENTING CYBER ATTACKS:

Banco Rabobank's information security monitoring process and the prevention against cyber-attacks consist of a set of detective and corrective controls, with the purpose of avoiding cybersecurity threats, among which the following stand out:

- Application of security updates and corrections;
- Monitoring against cyberattacks and prevention against invasion, as conducted by the Banco Rabobank Global team;
- Verification of safety requirements compliance;
- Periodic verification of vulnerabilities and management of vulnerabilities;
- Periodic testing and vulnerability scanning;
- Monitoring the status of anti-virus tools and alerts generated by them;
- Protection against malicious software;
- Prevention of information leakage.

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 Banco Rabobank 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 being made available in the productive environment ;
- Controls and traceability mechanisms;

o 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 General safety tests (such as safety parameters);

o 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. INFORMATION SECURITY TESTING

Bank Rabobank's information security testing management includes the following control mechanisms:

- Security testing for new applications;
- Security testing for existing applications;
- Follow up of corrections of failures appointed in tests;
- Execution of new testing to confirm that the failures have been corrected.

7. ACCESS CONTROL MANAGEMENT

The levels of control relied upon in the access control management of logical resources of Banco Rabobank vary according to the classification of the asset, including, among others, the following control mechanisms:

- Authentication controls;
- Cryptography;
- Authorization controls;
- Segregation of functions;
- Periodic review of accesses.

8. INFRASTRUCTURE / BUSINESS CONTINUITY MANAGEMENT

The primary objective of Bank Rabobank's controls in infrastructure development is to ensure that Banco Rabobank remains operational in the face of cyber threats in order to ensure the confidentiality, integrity and availability of information. At a minimum, the following controls must be adopted:

- Backup (safety copies) of data and information;
- Preparation of scenarios of incidents considered in the tests of business continuity, considering scenarios of unavailability caused by incidents of a cybernetic nature;
- The results of the business continuity tests must be informed for the preparation of the annual report on the action plan for incident response.

9. MANAGEMENT AND PLAN OF CYBERNETIC INCIDENTS RESPONSE

The management and plan of responses to cyber incidents for relevant services of Banco Rabobank must be performed considering the assessment of cause, impact and effect, as well as include the following controls:

- Incident Response Action Plan;
- Preventive, detective and mitigating measures of incidents related to the cyber environment;
- Processes and tools used to prevent and respond to incidents;
- Designation of the area responsible for recording and controlling the effects of relevant incidents;
- Record of incidents, with information about roles and responsibilities;
- Classification of the cybernetic incident;
- Cause and impact analysis;
- Receipt of supplier information related to incidents that have an impact on the provision of relevant services;
- Definition of mechanisms to prevent, detect and reduce vulnerability to incidents related to the cyber environment;
- Elaboration of the annual report on the action plan and incident response;
- Initiatives to share information about relevant incidents with other financial institutions authorized by the Central Bank of Brazil which occurred in Banco Rabobank and/or communicated by the relevant service providers;
- Timely communication to the Central Bank of the occurrence of relevant incidents and relevant service interruptions.

10.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, Banco Rabobank 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 Banco Rabobank's activities. Such controls must be compatible with the processes and cyber security mechanisms adopted by Banco Rabobank Bank.

11.CONTACT

If you have any questions regarding this document or the Cyber Security Policy ofBanco Rabobank, 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.

12.LEGAL NOTICE

This document was prepared by Banco Rabobank for informational purposes only. This document may not be reproduced (in whole or in part) for any other person without the prior formal authorization of Banco Rabobank.