INFORMATION SECURITY AND CYBERSECURITY SUMMARY POLICY

BEETELLER GROUP

Date 07.11.2022

Version [1.0]

1. Purpose

This Policy is a summary containing the general lines of the Information Security and Cyber Security Policy of BEETELLER GROUP, as per Article 4 of National Monetary Council (CMN) Resolution No. 4,893 of February 26, 2021. The Policy aims to establish standards, concepts, guidelines and responsibilities on the main aspects related to information security and cyber security, in order to preserve and ensure the confidentiality, integrity, availability and compliance of data and information of BEETELLER GROUP, customers, employees and the general public, observing the applicable regulations and best market practices.

2. Scope

All users, clients, employees, service providers, interested parties and of BEETELLER GROUP itself with access to any protected information or data of BEETELLER GROUP or that are under control or operation of BEETELLER GROUP, regardless oftheir bond with the company. It also applies to processes and technologies.

3. Commitment and Communication

BEETELLER GROUP Senior Management is committed to applying the best marketpractices and regulations in the aspects inherent to Information Security and Cybersecurity, promoting the continuous improvement of the procedures and controls present in this Policy. Furthermore, it undertakes to update the Policy annually or whenever necessary.

If there are indications of incidents, these should be reported to the Information Technology Department by e-mail: segurança.ti@beeteller.com. If necessary, the GROUP undertakes to forward this information to the competent bodies.

4. Guidelines

In order to ensure the goals and procedures of Information Security and Cybersecurity,this policy follows the following guidelines:

- Ensure that all information is treated ethically and confidentially, and that measures are taken to prevent improper access, modification, destruction, or unauthorized disclosure.
- Ensure that there is no undue access, modification, destruction or unauthorized disclosure of information. Any risk to information shall be immediately reportedby the Collaborator, service providers or Clients through the channels and procedures indicated by BEETELLER GROUP.
- Ensure that the information is used only for the purpose for which it was collected, and that access is conditional on authorization.
- Ensure that procedures and controls are adopted to reduce vulnerability to incidents and meet other Cybersecurity objectives, such as authentication, encryption, intrusion prevention and detection, information leak prevention, periodic testing and scanning for vulnerabilities, protection against malicious software, establishment of

traceability mechanisms, computer network accessand segmentation controls, and maintenance of backup copies of data and information.

- Ensure that specific controls, including those for information traceability, ensurethe security of sensitive information.
- Ensure that there is a risk management process in which they are mapped by analyzing vulnerabilities, threats, and impacts on information assets.
- Ensure that the incidents that occur are treated according to their criticality andimpact. Root cause analysis must be performed, and controls adopted to minimize the occurrence of new similar incidents.
- Ensure that every service that is fundamental to BEETELLER GROUP´s service delivery is contemplated with a continuity plan, to increase its operational resilience.
- Ensure that when using cloud computing services or hiring relevant vendors, BACEN's guidelines are observed.
- Ensure mechanisms for the dissemination of the cyber security culture, including the implementation of training programs and periodic evaluation of personnel.
- Ensure that all contracts observe the commitment to the Information Security and Cybersecurity Policy.

5. Final Provisions

All BEETELLER GROUP's employees, service providers, suppliers, providers and partners are committed to faithful compliance with this Security Policy in its entirety, always observing its most updated version.

Approved by: Lauriney Leite dos Santos Financial Director	Lauriney L. Santos Lauriney L. Santos (15 de Dezembro de 2022 13:06 GMT-3)
Approved by: Kelly Viviane da Silva Compliance & Risk Director	Kelly Viviane da Silva Kelly Viviane da Silva (15 de Dezembro de 2022 13:11 GMT-3)
Approved by: Caio Souza Vidal de Negreiros Chief Technology Officer	Caio S. Vidal Caio S. Vidal (15 de Dezembro de 2022 15:27 GMT-3)