CIELO S.A.
Corporate Taxpayer's ID (CNPJ /MF): 01.027.058/0001-91
Company Registry (NIRE): 35.300.144.112

EXCERPT OF THE MINUTES OF THE ORDINARY MEETING OF THE BOARD OF DIRECTORS HELD ON APRIL 26, 2021

(held via video conference)

Date, time and venue: April 26, 2021, at 1:30 p.m., at the head office of Cielo S.A. ("Company"), at Alameda Xingu, No. 512, 31º Andar, Alphaville, Centro Industrial e Empresarial, CEP 06455-030, in the city of Barueri, São Paulo state.

Presiding Board: Chair: Mr. Mauro Ribeiro Neto; Secretary: Ms. Tatiane Zornoff Vieira Pardo.

Attendance: A majority of the members of the Company's Board of Directors attended the meeting.

Call Notice: The meeting was duly called pursuant to article 17 of the Bylaws and items 4.3 and 4.4 of the Charter of the Board of Directors.

Agenda: **(1)** to analyze and resolve on the Company's Individual and Consolidated Interim Financial Information, accompanied by the Independent Auditor's Review Report of the Quarterly Information - ITR, referring to the first quarter of 2021, ended March 31, 2021; **(2)** to analyze and resolve on the proposal for declaration of interest on equity for the first quarter of 2021; and **(3)** to analyze and resolve on amendments to **(a)** the Anti-Money Laundering and Combating the Financing of Terrorism Policy and **(b)** the Information Security and Cybersecurity Policy.

Resolution: After the meeting was called to order, the members of the Board of Directors analyzed the items on the Agenda and resolved:

(1) **To approve**, by a unanimous vote, the Company's Individual and Consolidated Interim Financial Information, prepared in accordance with CVM regulations, accompanied by the unqualified Independent Auditor's Review Report of the Quarterly Information - ITR for the first quarter of 2021 (ended March 31, 2021) ("ITR 1Q"), as recommended by the Audit Committee.

The Company's Board of Executive Officers is authorized to take all necessary measures to disclose the 1Q ITR in the usual form.

(2) **To approve**, by a unanimous vote, in accordance with the recommendation of the Finance Committee and in compliance with article 31 of the Bylaws and the Company's Proceeds Policy, *ad referendum* of the Company's Annual Shareholders' Meeting to be held for the purpose of approving the result for fiscal year 2021, the declaration of interest on equity ("IoE"), in the total amount of eighty-five million, one hundred and fifty-one thousand, one hundred and twenty-one reais and twenty-one centavos (R$85,151,121.21), for the first quarter of 2021, subject to income tax, as applicable in each case. IoE will be distributed and paid to shareholders proportionally to their interest in the Company. Treasury shares will not be entitled to receive IoE.

This IoE, net of income tax, will be paid to shareholders on May 13, 2021, based on the shareholding position on April 30, 2021, and the Company's shares will be traded ex interest on equity as of May 3, 2021, inclusive.

Payment will be made through the Company's share depositary institution – Banco Bradesco S.A. ("Banco Bradesco"), via automatic credit to shareholders who have a Bradesco account and shareholders who have provided to Banco Bradesco their individual or corporate taxpayer's ID (CPF or CNPJ) and their respective bank details. Shareholders who have not provided this information should go to a Banco Bradesco branch to update their registration data. Shareholders whose shares are held in custody by B3 S.A– Brasil, Bolsa, Balcão will receive IoE through its custodial agents, and shareholders who own ADRs (American Depositary Receipts) will receive IoE through JP Morgan Chase Bank, the hired depository institution.

The Company's Board of Executive Officers is authorized to adopt all the procedures necessary to disclose these Minutes and notices to shareholders and ADR holders in the newspapers usually used by the Company, containing the necessary information, and communicate these data to the Brazilian Securities and Exchange Commission and B3 S.A. - Brasil, Bolsa, Balcão, as well as adopt all the necessary procedures for the payment of IoE.

(3) **To approve**, by a unanimous vote and in accordance with the recommendations of the Corporate Governance Committee, the Audit Committee and the Risks Committee, the proposed amendments to **(3.1)** the Anti-Money Laundering and Combating the Financing of Terrorism Policy and **(b)** the Information Security and Cybersecurity Policy, which will henceforth be worded as per Exhibits I and II.

Closing and Drawing up of the Minutes: There being no further matters to address, the meeting was adjourned for the time necessary to draw up these minutes, which were read, approved and signed by all those present.

Signatures: Presiding Board: Mr. Mauro Ribeiro Neto, Chair; Ms. Tatiane Zornoff Vieira Pardo, Secretary. Members of the Company's Board of Directors: Messrs. Mauro Ribeiro Neto, Marcelo de Araújo Noronha, Aldo Luiz Mendes, Carlos Motta dos Santos, Edson Marcelo Moreto, Edson Rogério da Costa, Francisco José Pereira Terra, Gilberto Mifano, Gustavo de Sousa Fosse and Vinícius Urias Favarão.

This is a free English translation of the minutes drawn up in the Company's records.

Barueri, April 26, 2021.

_____

TATIANE ZORNOFF VIEIRA PARDO
Secretary

(This is an integral part of the Excerpt of the Minutes of the Ordinary Meeting of the Board of Directors of Cielo S.A. held on April 26, 2021)

(The Exhibit I is an integral part of the Excerpt of the Minutes of the Ordinary Meeting of the Board of Directors of Cielo S.A. held on April 26, 2021)

POLICY

Title:	ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM	Code:	PLT_023
Board of Executive Officers:	Risk, Compliance, Prevention and Security	Version	04

Revision History

Version:	Revision Date:	History:
01	04/19/2018	Document preparation.
02	05/09/2019	In compliance with the Company's Normative Instruments standard, the policy has been reviewed, according to the rules set forth in said standard, and no need for changes to content has been identified. In this sense, the Board of Executive Officers became aware of the review conducted and, as this policy was not amended, it was not necessary to submit it to the Board of Directors.
03	04/23/2020	Annual review with the implementation of pertinent changes to the adequacy of processes, in line with the changes in the market and the regulations in force.
04	04/26/2021	General amendments to the content of sub-items of the Guidelines; Inclusion of items 1.2, 1.5, 1.8, 1.9 and 1.27. Changes to the working of the following items: Purpose, Scope, Responsibilities and Concepts and Acronyms. Inclusion of responsibilities for the Operations Superintendence.

Contents

I. Purpose

To set forth the guidelines to prevent and combat the crimes of money laundering and financing of terrorism, besides other crimes involving the simulation or concealment of funds, as provided for in the regulations of the Central Bank of Brazil ("BACEN"), the rules of the payment arrangement institutions ("Brands"), Law 9,613/1998 and guidelines in Cielo's Code of Ethical Conduct.

II. Scope

All management members (executive officers, members of the Board of Directors and members of the Advisory Committees), members of the Fiscal Council and employees of Cielo S.A., Servinet Serviços Ltda., Aliança Pagamentos e Participações Ltda. and Stelo S.A. ("Cielo" or "Company"), as well as their partners and outsourced service providers.

All Company subsidiaries must define their guidelines based on the guidance provided for in this Policy, considering the specific needs and legal and regulatory aspects to which they are subject.

Regarding its Affiliates, the Company's representatives acting as management members of the Affiliates must spare no effort for said companies to define their guidance based on the guidelines provided for in this Policy, considering the specific needs and legal and regulatory aspects to which they are subject.

III. Guidelines

1. Cielo:
   1.1. Repudiates money laundering, terrorist financing, corruption and any other illicit acts.
   1.2. Has a senior management team committed to the effectiveness and continuous improvement of the policy, procedures and internal controls related to the prevention of money laundering and financing of terrorism, as well as sends reports related to this process, whenever necessary, to the Board of Executive Officers and Board of Directors.
   1.3. Adopts a governance structure aimed at complying with this policy and the obligations related to the prevention of money laundering and the financing of terrorism, as per Law 9,613/1998 and the regulations of BACEN, through the creation of an Anti-Money Laundering Executive Working Group ("AML WG"), coordinated by the officer responsible for compliance of related obligations before BACEN.
   1.4. Adopts internal evaluation procedures, with the objective of identifying and measuring the risk of using its products and services and doing business related to money laundering and the financing of terrorism, in line with the national legislation and the rules of the payment arrangements to which it is a party, as per the responsibilities defined in internal regulations.
   1.5. Submits the internal risk assessment referred to in item 1.4 of this policy, approved by the officer responsible for the process of prevention of money laundering and the

financing of terrorism, to the Risks Committee, the Audit Committee and the Board of Directors, for information purposes, as well as reviews it every two years.

1.6. Adopts procedures to develop new products and services and use new technology in order to assess risk and prevent money laundering and the financing of terrorism, in accordance with the guidelines of the Corporate Risk Management and Internal Controls Policy and the responsibilities defined in internal regulations.

1.7. Annually assesses compliance with and effectiveness of this policy, procedures and internal controls, regarding prevention of money laundering and the financing of terrorism in order to identify possible deficiencies, in accordance with the guidelines of the Corporate Risk Management and Internal Controls Policy and the responsibilities defined in internal regulations.

1.8. Issues annual reports containing the results of the assessment of control effectiveness mentioned in item 1.7 of this policy, as well as submits it to the Audit Committee and the Board of Directors, for information purposes.

1.9. Adopts action plans to mitigate risks and correct the deficiencies identified in inspections carried out by Regulatory Bodies and Brands, as well as in assessments conducted by the Internal Controls and Internal Audit areas, aimed at checking the procedures to prevent money laundering and the financing of terrorism.

1.10. Adopts practices to promote an organizational culture of prevention of money laundering and the financing of terrorism.

1.11. Maintains a specific annual training program for employees on prevention and combat of money laundering and the financing of terrorism.

1.12. Adopts the Know Your Customer, Know Your Supplier, Know Your Partner and Know Your Employee due diligence procedures to mitigate risks related to money laundering and financing of terrorism, according to the activity, jurisdiction and the parties involved, including the collection, verification, validation and update of registration data, as defined in internal regulations.

1.13. Adopts restrictive measures as to the conduct of business and the maintenance of relationships with customers, suppliers and partners when circumstances indicate evidence of involvement in crimes of money laundering and financing of terrorism or any other illicit acts, according to prevailing laws.

1.14. Adopts procedures to identify customers, partners and outsourced service providers who may be included in restrictive lists, such as the lists issued by the U.S. Office of Foreign Assets Control (“OFAC”) and the United Nations Security Control (“UNSC”), among other lists of national and international administrative, social and environmental sanctions.

1.15. Immediately reports the identification of customers included in the OFAC and UNSC lists to the competent authority.

1.16. Adopts procedures to identify and approve the maintenance of business relationships with customers, partners and service providers who may be considered Politically Exposed Persons (“PEP”) or related to them, respecting due governance, as set out in internal regulations.

1.17. Devotes special attention to transactions or proposed transactions involving PEPs, as well as their family members, employees or legal entities in which they participate.

1.18. Adopts controls to certify that the settlement of transactions and fund transfers are carried out to checking accounts, savings accounts, prepaid cards and payment accounts (“digital wallet”) of customers affiliated with Cielo, whose identity and veracity have been previously confirmed.

1.19. Uses internal systems for recording and monitoring transactions, which, through parameterized rules, identifies cases with indication of money laundering or financing of terrorism and corruption, among other illicit activities.
1.20. Assesses, when analyzing transactions, the capture solution used, the form of payment, the frequency, the parties and the amounts involved, transaction patterns, economic activity and any other indication of irregularity or illegality involving the customer or its operations, aiming at detecting any indication of money laundering, financing of terrorism and corruption, among other illicit activities.
1.21. Maintains specific channels to receive reports, including anonymous reports, as well as repudiates any acts of reprisal or retaliation against the good-faith reporters who opted to identify themselves.
1.22. Analyzes indications and reports of practices connected with suspicious of money laundering and financing of terrorism by direct agents or third parties against Cielo's assets, according to prevailing laws.
1.23. Informs the appropriate authorities about transactions or proposed transactions with indication of money laundering, financing of terrorism and corruption, among other illicit acts, pursuant to prevailing laws.
1.24. Cooperates with public authorities in investigations related to money laundering, financing of terrorism and corruption, among other illicit acts resulting from its activities, according to prevailing laws.
1.25. Confidentially records, analyzes and communicates transactions with indication of money laundering or financing of terrorism to the appropriate authorities.
1.26. Established that any suspicious fact or indication of a direct or indirect connection with criminal acts, regardless of having been the purpose of the situations described above, shall be reported to the Compliance and Money Laundering Prevention areas.
1.27. Is committed to the continuous improvement of monitoring, selection, analysis and communication activities, reviewing and updating its processes, focusing on intelligence and technology.
1.28. Reviews the guidelines defined in this policy annually or whenever there are changes in the process that impact or justify its review.

IV. Communication Channels and Outcome Management

Employees, suppliers or other stakeholders who become aware of any non-compliance with the guidelines of this Policy may report it to the Ethics Channel, either anonymously or not, at:

- www.canalconfidencial.com.br/cielo
- Toll free: 0800 775 0808

Internally, those who do not comply with the guidelines of this Policy will be subject to accountability measures based on the seriousness of such non-compliance and in accordance with internal regulations.

V. Responsibilities

- **Management and Employees:** comply and ensure compliance with this Policy and, when necessary, consult the Risk, Compliance and Prevention Office about situations that involve conflict with this Policy or if the situations described herein occur.

- **Audit Executive Superintendence:** carry out independent and objective assessments of the quality and effectiveness of the policy, procedures and internal controls to prevent and combat money laundering and terrorism financing crimes.
- **People, Management and Performance:** support training and cultural actions, as well as the application of the criteria stipulated for hiring and employee conduct, focusing on preventing and combating money laundering and the financing of terrorism.
- **Operations Superintendence:** support the application of stipulated criteria, as set forth in internal regulations, for the registration and maintenance of customers, focusing on preventing money laundering and the financing of terrorism.
- **Efficiency and Procurement Superintendence:** support the application of stipulated criteria, as set forth in internal regulations, for the establishment and maintenance of business relationships, focusing on preventing money laundering and the financing of terrorism.
- **Risk, Compliance, Prevention and Security Office:** ensure compliance, based on the guidelines of this policy, with the requirements imposed by the regulations on the subject, in addition to keeping the content up-to-date and adherent, as well as evaluating its effectiveness and compliance.
- **Legal and Governmental Relations Superintendence:** inform the Risk, Compliance, Prevention and Security Office of updates on legal provisions and other duties, as set forth in internal regulations.
- **Anti-Money Laundering Executive Working Group ("AML WG"):** enforce compliance with the guidelines of this policy and the obligations set out in Law 9,613/1998 and BACEN regulations, as well as resolve on aspects related to the prevention of money laundering and the financing of terrorism.

VI. Additional Documentation

- BACEN Circular Letter 3,978/2020;
- BACEN Circular Letter 4,001/2020;
- Cielo's Code of Ethical Conduct;
- Anticorruption Policy;
- Compliance Policy;
- Law 9,613/1998;
- COAF Resolution 29/2017.

VII. Concepts and Acronyms

- **COAF (Financial Activities Control Council):** a council created within the Ministry of Finance with the purpose of disciplining, imposing administrative penalties, receiving, examining and identifying suspicion of illicit activities set forth in Law 9,613/1998, without prejudice to the competence of other agencies and entities.
- **AML WG:** Anti-Money Laundering Executive Working Group, responsible for governing the prevention of money laundering and the financing of terrorism, composed of the Risk, Compliance, Prevention and Security Officer; Fraud Prevention Manager; Compliance and Anti-Money Laundering Manager; and Anti-Money Laundering Coordinator.
- **OFAC (Office of Foreign Assets Control) list:** a list issued and regularly updated by the U.S. Treasury, containing names and associations of persons and companies restricted for connection with illicit acts such as drug trafficking, money laundering and terrorism, among others.

- **PEP (Politically Exposed Persons):** PEP refers to people who in the past five (5) years met the following conditions: (I) elective office in the federal government's executive and legislative branches; (II) a position at the Federal Executive Branch, serving as Minister (or a similar position) or holding a Special Nature position (or a similar position); (III) CEO, vice president and officer, or similar positions, at indirect government agencies; (IV) Senior Management and Advisory Group – DAS, level 6, or similar positions; (V) members of the National Council of Justice, Federal Supreme Court, Higher Courts and Federal Regional Courts, Labor and Electoral Courts, Superior Labor Justice Council and Federal Justice Council; (VI) members of the National Council of the Public Prosecution Office, Federal Attorney General, Vice Federal Attorney General, Labor Attorney General, Military Attorney General, Deputy Federal Attorney General and Deputy Attorney General of the States and Federal District; (VII) members of the Federal Accounting Court and the Attorney General and Deputy Attorneys General of the Public Prosecution Office in the Federal Accounting Court; (VIII) political party presidents or treasurers or similar positions; (VII) Federal District and state governors and secretaries, Federal District and state legislators, president (or a similar position) of entities of the state and district indirect government entities and presidents of Courts of Justice, Military Courts, Accounting Court or equivalent institutions in the States and the Federal District; (VIII) Mayors, City Counselors, Municipal Secretaries, presidents (or a similar position) of entities of the municipal indirect public administration and presidents of Municipal Accounting Courts or equivalent institutions. Politically exposed persons are also those who abroad are: (I) heads of state or government; (II) high-ranking politicians; (III) those holding high-ranking positions in the government; (IV) official generals and members of the judiciary, legislative branches or military high ranking; (V) top-level executives in state-owned companies; or (VI) leaders of political parties and leaders of state-owned companies (VII) leaders of high-ranking public or private international law entities.
- **Stakeholders:** all relevant public with interests relevant to the Company or individuals or entities that take some type of risk, direct or indirect, before society, such as shareholders, investors, employees, society, customers, suppliers, creditors, governments, regulatory bodies, competitors, press, associations and class entities, users of electronic payment methods and non-profit organizations, among others.

VIII. Miscellaneous

The Company's Board of Directors is responsible for amending this Policy whenever necessary.

This Policy will become effective as of its date of approval by the Board of Directors and revokes any documents, unless otherwise stated.

Barueri, April 26, 2021.

Cielo S.A.

The Exhibit II is an integral part of the Excerpt of the Minutes of the Ordinary Meeting of the Board of Directors of Cielo S.A. held on April 26, 2021)

POLICY

Title:	INFORMATION SECURITY AND CYBERSECURITY	Code:	PLT_012
Board of Executive Officers:	Risk, Compliance, Prevention and Security	Version	06

Revision History

Version:	Publication date:	History:
01	06/03/2014	Document preparation.
	11/13/2014	Given that there were no changes, the document has been revalidated for another two years by the Internal Control Officer, Mr. Eduardo Magalhães, therefore, no new version will be created.
02	06/26/2015	Inclusion of items Scope (II), Additional Documentation (III) and Miscellaneous (VIII); Update of items Concepts and Acronyms (IV), Responsibilities (V) and Consequence Management (VII).
03	07/07/2017	Update of items II. Scope, III. Additional Documentation, IV. Concepts and Acronyms and sub-items 1.2 and 1.4 of VI. Guidelines.
04	10/29/2019	Update of the Policy title to "Information Security and Cybersecurity". Amendment to items I. Purpose; II. Scope, III. Guidelines sub-items 1.1, 1.2, 1.3 and 1.4, V. Responsibilities, VI. Additional Documentation; VII. Concepts and Acronyms and VIII. Miscellaneous. Inclusion to item III. Guidelines, sub-items 1, 1.1.1, 1.1.2, 1.1.3, 2, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6,2.7, 2.8, 2.9, 2.10, 2.10.1, 2.10.2, 2.10.3 and 2.11.
05	06/29/2020	Amendment to items II. Scope; III. Principles, Rules and Procedures - sub-items 1.1.4, 1.4, 2., 2.1, 2.2; V. Responsibilities; VI Additional Documentation; and VII. Concepts and Acronyms. Inclusion of sub-items 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.1.5, 2.2.1, 2.2.2., 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.2.8, 2.2.9, 2.2.10, 2.2.11, 2.2.12, 2.2.13, 2.2.14, 2.2.15, 2.2.16 to item III. Principles, Rules and Procedures. Exclusion of sub-items 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.10.1, 2.10.2, 2.10.3, 2.11. in item III. Principles, Rules and Procedures.
06	04/26/2021	Update of sub-items 1.1.4, 1.1.5, 1.1.6, 1.2, 2.2.12, 2.2.15.2 of item III. Principles, Rules and Procedures. Amendments to items V. Responsibilities and VI. Additional Documents.

Contents

Title:	INFORMATION SECURITY AND CYBERSECURITY	Code:	PLT_012
Board of Executive Officers:	Risk, Compliance, Prevention and Security	Version	06

I. Purpose

Establish guidelines that allow Cielo SA ("Cielo" or "Company") to safeguard its information assets, guide the definition of specific rules and procedures for Information Security and Cybersecurity, and implement controls and procedures to reduce the vulnerability of Incidents.

II. Scope

All managers (members of the Board of Executive Officers, members of the Board of Directors and members of the Advisory Committees), members of the Fiscal Council, employees and service providers of Cielo S.A., Servinet Serviços Ltda., Braspag Tecnologia em Pagamentos Ltda., Aliança Pagamentos e Participações Ltda. and Stelo S.A., hereinafter referred to as ("Cielo" or "Company").

All Company subsidiaries must define their guidelines based on the guidance provided for in this Policy, considering the specific needs and legal and regulatory aspects to which they are subject.

Regarding its Affiliates, the Company's representatives acting as management members of the Affiliates must spare no effort for said companies to define their guidance based on the guidelines provided for in this Policy, considering the specific needs and legal and regulatory aspects to which they are subject.

III. Principles, Rules and Procedures

1. Regarding the information security:

1.1. guarantee information security, the Company carries out its activities based on the following pillars:

1.1.1. **Confidentiality:** ensure that the information will only be accessible to authorized persons;

1.1.2. **Integrity:** ensure that information, stored or in transit, will not undergo any unauthorized change, whether intentional or not;

1.1.3. **Availability:** ensure that the information will be available whenever necessary.

1.1.4. **Authenticity:** ensure that the information is from the original source and has not been altered.

1.1.5. **Irrevocability or non-repudiation:** guarantee that the legitimate author of the information cannot repudiate authorship, such as, for example, when accepting a digital contract using access credentials, it is understood that the acceptor cannot later deny his/her signature.

1.1.6. **Compliance:** ensure that the Company's processes are in accordance with the regulations, rules and laws in effect, in order to strictly follow all the protocols required in the sector in which the Company operates as a result of its activities.

1.2. Cielo considers that information assets is all information generated or developed for the business and can be present in the form of digital files, consent of customers and persons related to Cielo (opt-in and opt-out), equipment, external media, printed documents,

digitally signed documents, systems, mobile devices, databases, conversations and recordings.

1.3. The Company establishes that, regardless of the way presented, shared or stored, the information assets must be used only for their duly authorized purpose and are subject to monitoring and auditing.

1.4. Cielo establishes that all information assets owned by it must have a person in charge for them and must be duly classified based on criteria established in a specific regulation and properly protected from any risks and threats that may compromise the business.

2. General Cybersecurity Guidelines

2.1. With regard to cybersecurity, Cielo has the following general guidelines:

2.1.1. Safeguard data protection against unauthorized access, as well as against unauthorized modifications, destruction or disclosure;

2.1.2. Properly classify the information and guarantee the continuity of their processing, according to the criteria and principles provided for in the internal regulations in force on the matter;

2.1.3. Ensure that systems and data under its responsibility are properly protected and used only for the fulfillment of its duties;

2.1.4. Ensure the integrity of the technological infrastructure in which data is stored, processed or otherwise treated, adopting the necessary measures to prevent logical threats, such as viruses, harmful programs or other failures that may lead to unauthorized access, manipulation or use of internal and confidential data, through: **(i)** the maintenance of installed and updated antivirus and firewall software and **(ii)** the maintenance of computer programs installed in the environment, among others; and

2.1.5. Comply with the laws and rules that regulate Cielo's activities.

2.2. In order to comply with the guidelines listed above:

2.2.1. Cielo's cybersecurity purpose is to prevent, detect and reduce vulnerability to incidents related to the cyber environment.

2.2.2. With regard to security measures, Cielo adopts procedures and controls to reduce the Company's vulnerability to incidents and meet cybersecurity objectives, including: authentication, encryption, intrusion prevention and detection, prevention of information leakage, periodic testing and scanning to detect vulnerability, protection against malicious software, implementation of traceability mechanisms, access controls and segmentation of the computer network and the maintenance of backup copies of data and information, according to current internal regulations.

2.2.3. The Company controls, monitors and restricts access to information assets granting permission and privileges to the fewest people possible, pursuant to specific internal rules.

2.2.4. Cielo implements the procedures and controls mentioned above, including in the development of secure information systems and adoption of new technologies used in its activities.

2.2.5. The Company has specific controls, including those aimed at traceability of information, which seek to ensure the security of sensitive information.

2.2.6. Registering, analyzing the cause and impact and controlling the effects of incidents relevant to the Company's activities, including the information received from companies providing services to third parties.

2.2.7. Cielo prepares inventories of cyber crisis scenarios related to security incidents taken into consideration in continuity tests of payment services provided and carries out

annual tests to ensure the effectiveness of the processes, and prepares an annual incident response report in its technological environment.

2.2.8. Cielo classifies security incidents according to their relevance and to (i) the classification of the information involved; and (ii) the impact on the Company's business continuity, described in specific internal rules.

2.2.9. Cielo periodically assesses service provider companies that carry out the treatment of information relevant to the Company in order to monitor the maturity level of its security controls for the prevention and proper handling of incidents.

2.2.10. The Company has criteria for classifying the relevance of data processing and storage and cloud computing services, in Brazil or abroad, according to internal procedures.

2.2.11. Prior to contracting relevant data processing and storage and cloud computing services, the Company adopts the procedures set forth in specific BACEN regulations on the topic in effect.

2.2.12. Prior to contracting service providers that handle sensitive information or data or data that are relevant to the Company's operational activities Cielo evaluates whether they adopt procedures and controls aimed at the prevention and treatment of incidents in complexity, comprehensiveness and accuracy levels compatible with those adopted by Cielo.

2.2.13. It establishes rules and standards to ensure that information receives the appropriate level of protection as to its relevance, in accordance with internal regulations. All information has an owner, is mandatorily classified and receives the appropriate controls that guarantee its confidentiality, in accordance with good market practices and regulations in force.

2.2.14. The Company carries out actions to prevent, identify, record and respond to security incidents and crises that involve Cielo's technological environment and which may compromise the pillars of information security or generate image, financial or operational impact. The definition of relevance of incidents in the technological environment follows a corporate risk standards established in specific regulation.

2.2.15. It adopts mechanisms to disseminate the information security and cybersecurity culture at the Company, including:

2.2.15.1. The implementation of an annual training program for employees;

2.2.15.2. The implementation of a periodic assessment program for employees regarding their level of knowledge on the subject of information and cybersecurity;

2.2.15.3. The provision of information to end users on precautions in the use of products and services offered; and

2.2.15.4. Senior management's commitment to the continuous improvement of procedures related to information security and cybersecurity.

2.2.16. Cielo adopts initiatives to share information about significant incidents through membership in discussion forums.

IV. Outcome Management

Employees, suppliers or other stakeholders who see any deviations from the guidelines of this Policy may report the fact to the Ethics Channel (https://canaldeetica.com.br/cielo or 0800 775 0808), and may identify themselves or remain anonymous.

Internally, those who do not comply with the guidelines of this Policy will be subject to accountability measures based on the seriousness of such non-compliance.

V. Responsibilities

- **Management and Employees:** comply and ensure compliance with this Policy and, when necessary, contact the Vice-Presidency for Technology and Projects to get information on situations that relate to conflict with this Policy or with situations described herein. It is essential that each person understands the role of information security in their daily activities and participate in awareness programs.
- **Risk, Compliance, Prevention and Security Office:** comply with the guidelines established in this Policy and annually update it in order to ensure that any changes in Cielo's direction be included into it and clarify any doubts regarding its content and application.
- **Management, Employees, Suppliers and Contractors:** act in an ethical and responsible manner when becoming aware of incidents, sharing information with those responsible for dealing with such incidents in a timely manner and taking all the applicable actions to minimize potential damage, in accordance with the Incident Response Plan – CSIRT Cielo.
- **Board of Directors:** after prior assessment by the Advisory Committees, resolve on the annual approval of (i) the report on the implementation of the action and incident response plan to comply with Cielo's Information Security and Cybersecurity Policy and (ii) the Incident Response Plan – CSIRT Cielo.
- **Information Security and Fraud Prevention Manager Forum:** act proactively, supporting Information Security management by performing tasks related to the protection of Cielo's business and its customers' business.

VI. Additional Documentation

- Cielo's Code of Ethical Conduct
- Incident Response Plan – CSIRT Cielo
- PCI-Data Security Standard
- ABNT NBR ISO 27001 - Information Security
- BACEN Circular Letter 3909/18
- Internal standards and procedures constantly improved, approved by the competent levels and made available to all employees.
- Law 13,709, of August 14, 2018 - Brazilian General Data Protection Act (LGPD).
- Law 12,965, of April 23, 2014 – Brazilian Internet Framework;

VII. Concepts and Acronyms

- **Information Security:** Set of concepts, techniques and strategies that aim to protect Cielo's information assets.
- **Cybersecurity:** Set of technologies, processes and practices designed to protect networks, computers, systems and data from attacks, damages or unauthorized access.
- **Stakeholders:** Relevant public with interests relevant to the Company, as well as persons or entities that take some type of risk, direct or indirect, before the society. These include, among others, shareholders, investors, employees, society, customers, suppliers, creditors, governments, regulatory bodies, competitors, press, associations and class entities, users of electronic payment methods and non-profit organizations.
- **Affiliates:** companies in which the Company holds at least a ten percent (10%) interest on their share capital, without, however, controlling them, as per article 243, paragraph 1 of Brazilian Corporate Law.
- **Subsidiaries:** companies in which the Company, directly or indirectly, holds rights as a partner or shareholder that permanently ensure it preponderance in social resolutions and the power to elect the majority of managers, as per article 243, paragraph 2 of Brazilian Corporate Law.
- **Customers:** commercial establishments accredited to the Cielo System.

- **Data and/or Information:** all data referring to the activities carried out by Cielo in the performance of its corporate purpose, including data from Customers, personal or not, and classified according to the specific internal rule on the matter.
- **Incidents:** Any occurrence that actually or potentially compromises the confidentiality, integrity or availability of an information system or information that the system processes, stores or transmits or that constitutes violation or imminent threat of a breach of security policies, security procedures or acceptable usage policies.
- **Service Provider:** individual or legal entity, duly hired by Cielo to provide: (i) technology services; (ii) storage or any form of data and information treatment services; or (iii) who may have access, because of the scope of their contract, to confidential data, as classified in this Policy.
- **Cyber Risks:** risks arising from cyber attacks, originating from malware, social engineering techniques, invasions, network attacks (DDoS and Botnets) and external fraud, among others, that may expose Cielo's data, networks and systems, causing financial damage and/or significant reputation damages, which may impair the continuity of Cielo's activities.

VIII. Miscellaneous

The Company's Board of Directors is responsible for amending this Policy whenever necessary.

This Policy will become effective as of its date of approval by the Board of Directors and revokes any documents, unless otherwise stated.

Barueri, April 26, 2021.

Cielo S.A.