POLICY

Title	INFORMATION SECURITY AND CYBERNETICS	Code	PLT_012
VP/Board	Risks, *Compliance*, Prevention and Security	Version	08

Revision History

Version:	Approval Date:	History:
01	03/06/2014	Preparation of the Document.
	13/11/2014	Because there are no changes, the document was revalidated for another two years by the Director of Internal Controls, Mr. Eduardo Magalhães. Therefore, a new version will not be generated.
02	26/06/2015	Inclusion of items Scope (II), Complementary Documentation (III) and General Provisions (VIII); Update of items Concepts and Acronyms (IV), Responsibilities (V), and Consequence Management (VII).
03	07/07/2017	Update of items II. Scope, III. Supplementary Documentation, IV. Concepts and Acronyms and sub-items 1.2 and 1.4 of VI. Guidelines.
04	29/10/2019	Update in the title of the Policy for "Information Security and Cybernetics". Change of items I. Objective, II. Scope, III. Guidelines sub-items 1.1, 1.2, 1.3 and 1.4, V. Responsibilities, VI. Supplementary Documentation, VII. Concepts and Acronyms and VIII. General Provisions. Inclusion in 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	29/06/2020	Change to items II. Scope; III. Principles, Rules and Procedures - sub-items 1.1.4, 1.4, 2., 2.1, 2.2; V. Responsibilities; VI Supplementary 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 in 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	26/04/2021	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. Changes to items V. Responsibilities and VI. Supplementary Documentation.
07	20/04/2022	Update of items: I. Purpose, II. Scope, III.Principles, Rules and Procedures sub-items 1.1, 1.2, 1.2.5, 1.3, 1.5, 2, 2.1, 2.1.4, 2.2.1, 2.2.5, 2.2.6, 2.2.8, 2.2.12, 2.2.13, IV. Consequence Management, V. Responsibilities, VI. Supplementary Documentation and VII. Concepts and Acronyms.

08	03/29/2023	Update of items: I. Purpose, II. Scope, III. Principles Rules and Procedures sub-items: 1.2.6; 1.3; 2.1.2; 2.1.5; 2.2.10; 2.2.11 and 2.2.14. IV. Consequence Management, V. Responsibilities, VII. Concepts and Acronyms and VIII. General Provisions.
09	09/13/2023	It will be updated by Compliance, after final review.

Table of Contents

Title	INFORMATION SECURITY AND CYBERNETICS	Code	PLT_012
VP/Board	Risks, *Compliance*, Prevention and Security	Version	08

I. Purpose

This Information and Cyber Security Policy ("Policy") aims to establish guidelines to protect and safeguard information assets; guide the definition of specific standards and procedures for Information Security and Cybernetics; and implement controls and procedures to reduce the Company's vulnerability to incidents.

II. Scope

All members of the Board of Directors, Advisory Committees and Executive Board ("Officers"), members of the Fiscal Council; employees, including contractors, interns and young apprentices ("employees") of the companies Cielo S.A. – Instituição de Pagamento ("Cielo"), Servinet Serviços Ltda. ("Servinet"), Stelo S.A. ("Stelo"), and Aliança Pagamentos e Participações Ltda. ("Aliança"), hereinafter jointly referred to as "Company".

All the Company's Subsidiaries must define their directions based on the guidelines set forth in this Policy, considering the specific needs and the legal and regulatory aspects to which they are subject.

With respect to the Affiliates, the Company's representatives who act in managing its Affiliates must make every effort to define their directions based on the guidelines set forth in this Policy, considering the specific needs and the legal and regulatory aspects to which they are subject.

III. Principles, Rules and Procedures

1. On Information Security and Cybernetics

1.1. The Company aims to develop processes and products considering the pillars and good information security practices, supported by the management of cyber risks as a strategic subject to the business, and to promote the security culture among all employees to prevent, detect and reduce vulnerability to incidents related to the cyber environment.

1.2. The Company establishes the following pillars:

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

1.2.2. **Integrity**: ensure that the information handled, stored or transmitted will not undergo any unauthorized modification, whether intentional or unintentional;

1.2.3. **Availability**: ensure that the information is available whenever necessary.

1.3. For the development of the Company's products and processes, the following principles are considered:

1.3.1. **Authenticity**: Ensure that the information comes from the original source and has not been changed.

1.3.2. **Irretraction or non-repudiation**: ensure that the legitimate author of the information cannot deny his authorship.

1.3.3. **Compliance**: ensure that the Company's processes are in accordance with the regulations, standards and applicable laws in force, in order to strictly follow all protocols required in its operating sector.

1.4. The Company considers information assets to be all those generated or developed for the business, such as consents from customers and persons connected with the Company (opt-in and opt-out), registration data of clients and employees, payment information and the holders of these means of payment, as well as conversations and recordings with clients. Information assets can be present in many forms, such as digital files, external media, printed documents, digitally signed documents, mobile devices, databases, and audio recordings.

1.5. Information assets, regardless of the form presented, shared or stored, should be used only for their authorized purpose, and are subject to monitoring and auditing.

1.6. A person in charge must be assigned to all information assets, which must be classified according to their level of confidentiality, based on the criteria established in a specific standard, and adequately protected from any risks, as well as from threats that may compromise the Company's business.

1.7. The Information Security and Privacy Management System (SGSPI), for the scope established in a specific document, was implemented considering the regulatory requirements of ABNT NBR ISO/IEC 27001:2022 and ISO/IEC 27701:2020 and adequate governance structure already existing in the Company. The process is structured on the model of continuous improvement, providing a constant evolution of information security and privacy issues, and aligned with the guidelines set out in this document. The definitions on the matter, as well as the roles and responsibilities, are formalized in the Security and Privacy Management System ("SGSPI") Handbook.

2. General Guidelines for Information Security and Cybernetics

2.1. The Company's general guidelines are:

2.1.1. Safeguard the protection of data against undue access, as well as against modification, destruction or unauthorized disclosure;

2.1.2. Perform the proper classification of the information and ensure the continuity of its processing, according to the criteria and principles indicated in the internal regulations;

2.1.3. Ensure that the 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 its technological infrastructure in which data is stored, processed or otherwise handled, taking the necessary measures to prevent logical threats such as viruses, harmful programs or other failures

that may cause unauthorized access, handling or use to internal and confidential data.

2.1.5. Ensure that interventions carried out in the technological environment, such as audits, security tests or other activities in the environment that may in some way impact the operating systems or business processes, are previously agreed between the applicant and the person responsible for the environment.

2.1.6. Comply with the laws and standards that regulate its activities.

2.2. In order to comply with the above guidelines, the Company:

2.2.1. Adopts security procedures and controls to meet cybersecurity objectives, including: authentication, encryption, intrusion prevention and detection, information leak prevention, periodic testing and scanning for vulnerability detection, protection against malicious software, establishing traceability mechanisms, access controls, segregation of duties, segmentation of the computer network and the maintenance of backup copies of data and information, in accordance with internal regulations.

2.2.2. Controls, monitors, restricts access to information assets to the lowest possible permission and privileges, as described in NRM_065 Logical Access and Digital Identity Management internal policy.

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

2.2.4. Has specific controls, including those aimed at the traceability of information, which seek to ensure the security of sensitive information.

2.2.5. Carries out actions to prevent, identify, record and respond to security incidents and crises that involve its technological environment and that may cause the compromise of information security pillars or generate an impact on its image, whether financial or operational.

2.2.6. Classifies information security and cyber incidents according to their relevance and according to (i) the classification of the information involved; and (ii) the impact on the continuity of the Company's business, as described in specific internal standards. The definition of relevance of incidents in the technological environment follows the corporate standard of risks established in internal standard NRM_124 Non-Financial Risk Management.

2.2.7. Records, analyzes the cause and impact, as well as the control of the effects of incidents relevant to the Company's activities, which include information received from companies providing services to third parties.

2.2.8. Establishes and documents in internal regulations the criteria that configure crisis situations, and prepares an inventory of cyber crisis scenarios related to security incidents considered in the continuity tests of payment services provided, and conducts annual tests to ensure the effectiveness of the processes, in addition to producing an annual incident response report in the technological environment.

2.2.9. Has criteria for classifying the relevance of data processing and storage and cloud computing services, in the country or abroad, according to internal procedure.

2.2.10. Prior to contracting relevant data processing and storage and cloud computing services, the procedures established in the regulations of the Central Bank of Brazil ("BCB") will be adopted.

2.2.11. Prior to hiring service providers that handle sensitive data or information or that are relevant to the conduct of the Company's operational activities, evaluates whether procedures and controls are adopted aimed at preventing and handling incidents at levels of complexity, scope and accuracy compatible with those adopted by the Company for the type of service rendered.

2.2.12. Performs the periodic evaluation of service providers that handle information relevant to the Company in order to monitor the level of maturity of its security controls, including those used for the prevention and proper handling of incidents.

2.2.13. Adopts initiatives to share information about relevant incidents through participation in discussion forums.

2.2.14. Establishes rules and standards to ensure that information receives the appropriate level of protection as to its relevance as per internal regulations. All information has an owner, is classified and receives the appropriate controls to ensure confidentiality, in line with the good market practices and regulations in force.

2.2.15. Adopts mechanisms for the dissemination of the Company's information security and cybersecurity culture, including:

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

2.2.15.2. The implementation of a program for periodic evaluation of employees to determine the level of knowledge on information security and cybernetics;

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

2.2.15.4. The commitment of management to the continuous improvement of procedures related to information security and cybernetics.

IV. Consequence Management

Employees, vendors or other stakeholders who observe any deviations from the guidelines of this Policy may report the fact to the Ethics Channel through the channels below, with the option of anonymity:

- https://canaldeetica.com.br/cielo
- Phone, toll-free: 0800 775 0808

Internally, non-compliance with the guidelines of this Policy gives rise to the application of accountability measures to the agents that fail to comply with it, according to the respective severity of the non-compliance and as per internal regulations, and is applicable to all persons described in the item "Scope" of this Policy, including the leadership and members of the Executive Board.

V. Responsibilities

- **Officers, Employees and Service Providers:** Observe and ensure compliance with this Policy and, when necessary, call the Vice Presidency of Risks, Compliance, Prevention and Security for consultation on situations involving conflict with this Policy, or upon the occurrence of situations described herein. Act ethically and responsibly when aware of incidents, sharing information with those responsible for handling it and taking all appropriate actions to minimize potential damages, according to the Incident Response Plan - CSIRT Cielo. Understand the role of information security in their daily activities and participate in awareness programs, as well as contributing to the implementation, maintenance and continuous improvement of the ISPMS.
- **Executive Board:** To decide, as recommended by the Information Security and Fraud Prevention Management Forum, on the resources for implementing, maintaining and improving the Information Security and Privacy Management System (SGSPI), as well as carrying out periodic critical analysis of the system, assessing the results, metrics and indicators, in addition to promoting the relevance of the Information Security and Privacy Management System (SGSPI) to all employees.
- **Vice Presidency of Risks, Compliance, Prevention and Security**: Comply with the guidelines set forth in this Policy, keep it updated to ensure that any changes to its guidance are incorporated hereto, and clarify doubts regarding its content and application.
- **Board of Directors**: After issuing a favorable recommendation by the competent Advisory Committees, deliberate annually on the following: (i) report on the implementation of the action plan and incident response for compliance with the Company's Information and Cyber Security Policy, and (ii) Incident Response Plan – CSIRT Cielo.
- **Information Security and Fraud Prevention Managing Forum:** Acting proactively, supporting Information and Cyber Security management in fulfilling the tasks related to protecting the Company's business and its clients, as well as advising the Executive

Board on the issues within its purview. Members must promote the relevance of the SGSPI in the company, acting as ambassadors for the subject in their respective areas, as well as carrying out periodic critical analysis of the system and other related activities.

- **Vendors**: Observe and ensure compliance with the best information security practices, as well as the information security and cybersecurity requirements contractually required while associated with the Company. Act ethically and responsibly when aware of incidents, sharing information with those responsible for handling it and taking all appropriate actions to minimize potential damages, according to the Incident Response Plan - CSIRT Cielo.

VI. Supplementary Documentation

- ABNT NBR ISO 27001 - Information Security.
- Cielo's Code of Ethics
- Law No. 12.965 dated April 23, 2014 - Internet Civil Framework.
- Law No. 13.709 dated August 14, 2018 - General Data Protection Law ("LGPD").
- Internal standards that are constantly improved, approved by the competent approval authority, and provided to all employees.
- *PCI DSS Payment Card Industry Data Security Standard.*
- Incident Response Plan - CSIRT Cielo.
- Corporate Business Continuity Management Policy.
- BCB Resolution No. 85/21.
- BCB Circular Letter No. 3,909/18.
- Rules of Procedure of the Information Security and Fraud Prevention Management Forum.

VII. Concepts and Acronyms

- **Clients:** Individuals or legal entities that use the products and/or services offered by the Company.
- **Board of Directors:** a collegiate decision-making body that aims to satisfy the duties of guiding and supervising the management of the Executive Board and deciding on major business issues, including making strategic, investment, and financing decisions, among other matters provided for in article 142 of the Brazilian Corporation Law and/or the Company's Bylaws.
- **Advisory Committees:** advisory bodies to the Board of Directors, of a technical nature, which are instruments of support and which increase the quality and efficiency of the performance of the Company's Board of Directors. The Advisory Committees have no deliberative power and their recommendations are not binding on the Board of Directors.

- **Data and/or Information:** all data relating to the activities developed by the Company in the execution of its corporate purpose, including client data, personal or otherwise, classified according to the specific internal standard on the subject.
- **Executive Board:** the body responsible for managing the company's business, executing the strategy and general guidelines approved by the Board of Directors. Through formalized processes and policies, the Executive Board enables and disseminates the Company's purposes, principles, and values.
- **Information Security and Fraud Prevention Managing Forum:** A collegiate technical body linked to and advising the Executive Board on matters related to information and cyber security management, with a view to complying with the legislation applicable to the subject, as well as protecting the Company's business and that of its clients.
- **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 constitutes an imminent breach or threat of breach of security policies, security procedures, or acceptable usage policies.
- **Significant Influence:** the power to participate in the financial and operational decisions of an entity, but that does not necessarily characterize control over these policies. Significant Influence can be obtained through ownership interest, statutory provisions, or a shareholders' agreement. When an investor directly or indirectly holds twenty percent or more of the voting power of an investee, it is presumed to have significant influence, unless it can be clearly demonstrated otherwise. The existence of significant influence may also be evidenced in one or more of the following ways: (i) representation on the board of directors or executive board of the investee; (ii) participation in policy-making processes, including in decisions about dividends and other distributions; (iii) material transactions between the investor and the investee; (iv) exchange of directors or managers; (v) provision of essential technical information.
- **Service Provider:** natural or legal person, duly contracted by the Company, providing services involving: (i) technology; (ii) storage or any form of processing of Data and Information; or (iii) that will have access to Confidential Data, due to the scope of the contract, as classified in this Policy.
- **Cyber Risks:** risks of cyber attacks arising from *malware*, social engineering techniques, intrusions, network attacks (DDoS and Botnets), external fraud, among others, that may expose the Company's Data, networks and systems, causing considerable financial and/or reputational damage, and may, in some circumstances, impair the continuity of the Company's activities.
- **Information Security:** set of concepts, techniques and strategies aiming to protect the Company's information assets.
- **CyberSecurity:** set of technologies, processes, and practices designed to protect networks, computers, systems, and data from attacks, damage, or unauthorized access.
- **SGSPI:** Information Security and Privacy Management System.

- ***Stakeholders:*** all relevant target audiences with interests pertinent to the Company, as well as individuals or entities that assume some type of risk, direct or indirect, with respect to the Company. Among others, the following are highlighted: shareholders, investors, employees, society, clients, vendors, creditors, governments and regulatory bodies, competitors, press, associations and class entities, users of electronic means of payment, and non-governmental organizations.
- **Affiliates:** companies in which the Company has a significant influence.
- **Subsidiaries:** companies in which the Company, directly or indirectly, holds partner or shareholder rights that assure it, on a permanent basis, preponderance in the corporate deliberations and the power to elect the majority of the officers, under the terms of current legislation.
- **Incident Response Plan - CSIRT Cielo.** Procedure established so that information security and cybersecurity incidents are identified and responded to in accordance with internally established guidelines.
- Opt-In**:** Option to receive information, contacts, or subscribe to services.
- Opt-Out**:** Option not to receive information, contacts or unsubscribe from services.

VIII. General Provisions

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

This Policy takes effect on the date of its approval by the Board of Directors and revokes any documents to the contrary.

Barueri, September 13, 2023.

Cielo S.A. – Instituição de Pagamento