INFORMATION SECURITY AND CYBERSECURITY POLICY

PAGSEGURO INTERNET INSTITUIÇÃO DE PAGAMENTO S.A.
AND OTHER COMPANIES OF THE PRUDENTIAL CONGLOMERATE

The **Information Security and Cybersecurity** guidelines of **PagSeguro Internet Instituição de Pagamento S.A.** ("PagBank"), the leader of the Prudential Conglomerate, **BancoSeguro S.A.** ("BancoSeguro") and **PagInvest Corretora de Titulos e Valores Mobiliarios Ltda** ("PagInvest"), institutions belonging to the Prudential Conglomerate of PagSeguro, collectively referred to as "Companies", fully adhere to the commitment of the Companies' Senior Management, aligned with the strategic objectives of their businesses, to ensure the application of principles for protecting the information of their clients, partners, third parties, professionals, or any institution or person in a relationship with the Companies.

These guidelines serve as the foundation for meeting and controlling Information Security and Cybersecurity Governance processes to:

- Preserve the **confidentiality, integrity, availability**, authenticity, and other security attributes of information owned and/or under its custody, avoiding exposure and providing appropriate protection;
- Establish guidelines for the **classification of data and information** through criteria and restrictions for accessing, processing, or transmitting confidential, sensitive, or restricted information of the Companies or their clients that has not been authorized by the responsible party;
- Implement procedures and controls to mitigate vulnerabilities, incidents, and security risks, signal the health of the environment, and produce remediation and/or containment plans, security risk generation, and information about the situation and status of assets in response to concerns and threats according to the Companies' risk appetite and strategies, thus reducing attacks and associated risks;
- **Manage, identify, respond to, treat, and reduce information security incidents**, as well as proactively monitor, detect, and investigate such occurrences through threat intelligence, and communicate and/or share (when applicable and especially in the case of significant incidents) with involved areas, regulatory bodies, intelligence partners, and external entities;
- Provide mechanisms for preventing data and information leakage (Data Loss Prevention – DLP) to detect possible violations or patterns of conduct that may infringe on the Companies' regulations;
- Offer protection mechanisms through the monitoring of endpoint activities, sensors, and hardware or software protection controls against malicious code that, once executed, could infiltrate or cause damage to the Companies' networks or assets;
- Provide guidelines for the use of network resources or, in a broader context, computational resources, whether fixed assets and/or removable mobile devices, aiming for best practices in handling, protection, processing, monitoring, and sharing of information;

- Provide plans and sub-plans (Business Impact, Operational Continuity, Business Recovery, Incident Management, Crisis Management, and Test/Validation Plans) for recovering critical services to ensure operational availability and **business continuity**, as well as operational procedures to reduce the impacts resulting from service interruption caused by disasters, crises, unavailability, failures, compromises, or significant security events;
- Manage and monitor Access Control, whether physical and/or logical, to information and assets, as well as their storage, sharing, and disposal, so that only authorized personnel can use them under rules, permissions, profiles, and/or corporate policies;
- Establish secure criteria for the use and maintenance of credentials, secrets, tokens, and passwords in the context of using corporate systems;
- Inform professionals, users, service providers, clients, and partners that:

○ it is not allowed to remove security controls or applications used for information access or protection, nor make changes to the production environment without previous approval;
○ media, equipment for accessing information systems, and complementary infrastructures are owned by the Company and subject to monitoring. Internet content access and email use are the responsibility of the account holder, service provider, client, or partner, subject to the application of current government laws, decrees, and regulations; and
○ the use of any technological resource or proprietary information for illegal actions is not permitted, nor is the installation of unauthorized computational resources.

- Define fundamental controls for the secure lifecycle and development of software, the use of new technologies that can guide projects within the context of secure software;
- Assist in scaling security requirements based on reference architecture, the use of cryptographic controls, and necessary protections according to the complexity and security level required for each component;
- Ensure that internally developed systems or those acquired from suppliers comply with security standards and best practices defined by the market or business needs;
- Establish guidelines for maintaining backup and restore copies of data and information for the Companies' official repositories and storage locations, as well as regulations for information retention and logging, in compliance with regulatory bodies and current legal matters;
- Continuously disseminate, at all levels and spheres, and to the widest possible audience, internally and/or externally (to clients) when applicable, **awareness programs and actions, training, acculturation, and prevention** regarding Information Security and Cybersecurity;
- Analyze, approve, and classify contracts, under current legislation and from the perspective of Information Security, whether for the hiring of relevant (or non-relevant) processing, storage, or cloud services; and
- Support risk issues by providing a common, integrated, and continuous risk model and process for identifying, analyzing, evaluating, treating, reviewing, and communicating

mapped risks in order to protect the companies' assets during assessment and control definitions that can validate the scope of this policy to assess the security level of information security controls in response to demanding areas (Internal Audit, Internal Controls, and Compliance).

The violation of security control or non-compliance with guidelines is considered an offense and may result in disciplinary measures (sanctions) to be validated by the Human Resources, Legal, Compliance, and Information Security departments of PagBank, according to their nature and frameworks provided in current laws.

PAGSEGURO INTERNET INSTITUIÇÃO DE PAGAMENTO S.A.