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

B. Scope All employees, including outsourced personnel, interns, and young apprentices ("employees") of Beephish Treinamento e Capacitação LTDA.

C. Principles, Rules, and Procedures

1. About Information and Cybersecurity

1.1. The Company aims to develop processes and products considering the pillars and good practices of information security, supported by the management of cyber risks as a strategic business matter, and to foster a 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:** ensuring that information will only be accessible to authorized persons;

1.2.2. **Integrity:** ensuring that information, processed, stored, or transmitted, will not suffer any unauthorized modification, whether intentional or not;

1.2.3. **Availability:** ensuring that information will be available whenever necessary.

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

1.3.1. **Authenticity:** ensuring that the information originates from the original source and has not been tampered with;

1.3.2. **Irreversibility or Non-repudiation:** ensuring that the legitimate author of the information cannot deny its authorship;

1.3.3. **Compliance:** ensuring that the Company's processes are in accordance with applicable regulations, norms, and laws, in order to strictly follow all protocols required in its sector of activity.

1.4. The Company considers information assets to be all those generated or developed for the business, such as client and Company-related person consents (opt-in and opt-out), client and employee registration data, as well as conversations and recordings with clients. Information assets can be present in

various 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, must be used only for their duly authorized purpose, being subject to monitoring and auditing.

1.6. A responsible party must be assigned to every information asset, which must be duly classified according to its level of confidentiality, in accordance with the criteria established in specific norms, and adequately protected from any risks, as well as threats that may compromise the Company's business.

2. General Information and Cybersecurity Guidelines

2.1. The Company has the following general guidelines:

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

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

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

2.1.4. Ensure the integrity of its technological infrastructure where data is stored, processed, or otherwise handled, adopting the necessary measures to prevent logical threats, such as viruses, malicious programs, or other failures that may cause unauthorized access, manipulation, or use of 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 operational systems or business processes, are previously agreed upon between the requester and the responsible party for the environment.

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

2.2. In view of complying with the guidelines listed above, the Company:

2.2.1. Adopts security procedures and controls to meet cybersecurity objectives, including: authentication, encryption, intrusion prevention and detection, information leakage prevention, periodic tests and scans for vulnerability detection, protection against malicious software, establishment of traceability mechanisms, access controls, segregation of duties, computer network

segmentation, and maintenance of data and information backups, as per internal norms.

2.2.2. Controls, monitors, and restricts access to information assets to the lowest possible permission and privileges, as described in internal norms.

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

2.2.4. Has specific controls, including those aimed at information traceability, 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 involving its technological environment that may cause the compromise of its information security pillars or generate image, financial, or operational impact.

2.2.6. Classifies information and cybersecurity incidents according to their relevance and in accordance with (i) the classification of the information involved; and (ii) the impact on the continuity of the Company's business, as described in specific internal norms.

2.2.7. Records, analyzes the cause and impact, as well as controls the effects of incidents relevant to the Company's activities, which include, among others, information received from third-party service providers.

2.2.8. Establishes rules and standards to ensure that information receives the appropriate level of protection regarding its relevance, as per internal norms. All information has an owner, is classified, and receives the proper controls, which guarantee its confidentiality, consistent with market best practices and current regulations.

2.2.9. Adopts mechanisms for disseminating the information and cybersecurity culture within the Company, including:

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

2.2.9.2. The implementation of a periodic employee evaluation program to assess the level of knowledge regarding information and cybersecurity;

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

2.2.9.4. The administration's commitment to the continuous improvement of procedures related to information and cybersecurity.

D. Consequence Management Non-compliance with the guidelines of this Policy entails the application of accountability measures to the agents who fail to comply, according to the respective severity of the non-compliance and in accordance with internal norms, being applicable to all persons described in the "Scope" item of this Policy.

E. Responsibilities

- **Administrators, Employees, and Service Providers:** Observe and ensure compliance with this Policy. Act ethically and responsibly when becoming aware of incidents, sharing information with those responsible for their treatment and taking all appropriate actions to minimize potential damages, in accordance with the Incident Response Plan procedure. Understand and perform the role of information security in their daily activities.

F. Complementary Documentation

- ABNT NBR ISO 27001 - Information Security.
- Law No. 12.965, of April 23, 2014 – Brazilian Civil Rights Framework for the Internet.
- Law No. 13.709, of August 14, 2018 - General Data Protection Law ("LGPD").

G. General Provisions This Policy comes into effect on the date of its publication and revokes any contrary documents.

São Paulo, August 01, 2024

Beephish Treinamentos e Capacitação LTDA.