PRIVACY AND INFORMATION SECURITY POLICY

I – INTRODUCTION:

1.1 This PRIVACY AND INFORMATION SECURITY POLICY is intended to establish the corporate rules and standards that must be observed for the management and protection of data and information within physical and technological environments.

1.2 While Privacy focuses on protecting the collection, sharing, and use of data and information, and Security seeks to protect such data and information against cyberattacks, we understand that both policies — Privacy and Security — may be addressed together, as they essentially share the common objective of protecting data and information related to the execution of ZOOMHOLDING's business activities.

1.3 ZOOMHOLDING is committed to protecting the data and information of its employees, clients, service providers, and any third parties interacting with its clients. Therefore, compliance with this Policy is mandatory, in accordance with Law No. 13,709/2018 (Brazilian General Data Protection Law – LGPD) and other applicable regulations.

II – INTRODUCTORY PROVISIONS:

2.1 The rules set forth in this Policy apply to all officers, representatives, employees, and service providers who interact with ZOOMHOLDING, directly or indirectly, in the performance of the services provided by ZOOMHOLDING.

2.2 For the purposes of this Policy, the following definitions shall apply:

2.2.1 Information Technology Team: ZOOMHOLDING's team responsible for the support and maintenance of its server and all operating systems used by ZOOMHOLDING;

2.2.2 Employee: the professional hired by ZOOMHOLDING to provide services either under an employment relationship or under a service provision relationship, in cases of outsourcing permitted by law.

2.3 The duty of confidentiality regarding confidential data and information to which employees, representatives, and service providers had access during the period in which they maintained contractual relationships with ZOOMHOLDING shall be maintained indefinitely, both during and after termination of the contractual relationship, under penalty of being held liable for damages caused by the disclosure of confidential information.

2.4 For the purposes of the preceding clause, any information to which the employee has access as a result of the performance of their duties and activities, whether oral or written, transmitted through physical or electronic documents, of a technical, commercial, tax, financial, personal, or any other nature, even if not specified herein, shall be deemed confidential and may only be disclosed with the prior written consent of the data subject or owner of the confidential information, or pursuant to a court order, or further in compliance with a legal obligation.

III – DATA PROCESSING:

3.1 ZOOMHOLDING does not use its clients' data, whether from individuals or legal entities, for advertising campaigns, digital marketing, or any other activity of a similar nature.
3.2 Data processing means any activity that uses personal data in the execution of its operations.
3.3 At ZOOMHOLDING, data processing is always carried out due to contractual and legal obligations. Therefore, although there is no sharing of data for marketing or commercialization purposes, ZOOMHOLDING may share personal data of clients, its employees, and third parties linked to its clients with tax authorities and Public Administration bodies, whether direct or indirect, Boards of Trade or delegated authorities, for the purposes of registering companies with the Commercial Registry or with Registry Offices of Deeds and Documents, complying with labor and tax obligations, whether ancillary or principal, and also providing information required by law, regardless of the data subject's consent, such as IBGE, COAF declarations, among others.
3.3.1 Employees and the Information Technology Team may have controlled access to data, whether personal or not, stored by ZOOMHOLDING.
3.4 The sharing of data outside the cases provided for in the preceding clause, namely clauses 3.3 and 3.3.1, is prohibited and may only occur in the situations set forth below, always observing the principles of purpose limitation, adequacy, necessity, transparency, and other applicable principles:

a) with the express consent or at the request of the data subject;
b) in situations aimed at satisfying the client's interests, such as providing the name and telephone contact to suppliers or third parties who may assist the client in the proper performance of their activities, provided that prior consent has been obtained;
c) when necessary to comply with a legal obligation;
d) pursuant to a court order.

3.5 Personal data may be stored electronically during and after the contractual relationship, for as long as the service provided may be subject to judicial challenge.
3.6 Our employees, clients, suppliers, and third parties interacting with our clients have the right to request correction whenever they identify any error, inaccuracy, or outdated information regarding their personal data.
3.7 The deletion of personal data of any person interacting with ZOOMHOLDING may be requested, provided that the stored data is not subject to the retention period established for compliance with a legal or regulatory obligation, or for the purpose provided for in clause 3.5.

IV – DATA AND INFORMATION SECURITY:

4.1 The security of the data processed by ZOOMHOLDING is of utmost importance. We adopt all appropriate measures to minimize potential risks and protect the data we store. Our procedures are subject to constant review and monitoring.
4.2 The use of information technology and communication equipment, systems, and information for employees' personal activities is not permitted, except in personal situations that are essentialto

ensuring the health and physical integrity of the employee or their family members, or when related to constitutionally guaranteed fundamental rights.

4.3 The use of passwords is personal and non-transferable, and each employee is responsible for keeping and safeguarding their passwords. Passwords must be changed immediately in the event of any suspicion of breach, in which case the employee must also immediately report the matter to the Information Technology Team.

4.3.1 As a measure to resist malicious attacks, passwords used to access ZOOMHOLDING's server, software, systems, and e-mail accounts must:

a) use different codes for each system;

b) contain the maximum number of characters allowed;

c) be heterogeneous and combined, using numbers, symbols, uppercase and lowercase letters;

d) never match other passwords used for personal purposes, such as banking or website registrations;

e) be changed periodically, in compliance with the requirements set forth above.

4.3.2 Whenever a new system is configured, any password that may have been factory-set or sent by e-mail must be changed immediately.

4.4 The collection of client data for compliance with accounting, tax, and employment obligations must preferably be carried out electronically, by e-mail or through a platform made available by ZOOMHOLDING. The sending and receipt of documents by any other means may only be used when requested by the client, in which case the client shall be responsible for information security.

4.5 Any and all incidents affecting information security must be immediately reported to the Information Technology Team.

4.6 Physical documents sent by clients or employees must be digitized in a technologically secure environment, whether on the server or in the cloud, and not on a local machine. ZOOMHOLDING shall store physical documents for as long as necessary to comply with its legal obligations.

4.7 The photographic reproduction of documents containing personal data is prohibited. The occasional reproduction of documents that do not contain personal data is permitted solely and exclusively for the purpose of better performing accounting and administrative entries, and such documents must subsequently be destroyed through a shredding process. The use of copies as drafts or for any other purpose unrelated to the performance of the services provided by ZOOMHOLDING is prohibited.

4.8 Users must log out of any program or platform on the internet, cloud server, e-mail account, server, or any operating system that requires a user login and password, using the appropriate logout field.

V – COMPUTERS, E-MAIL, INTERNET, AND TECHNOLOGICAL RESOURCES:

5.1 Each employee who uses electronic and information technology equipment, systems, and operating software is responsible for complying with the guidance provided by the Information Technology Team, and must not run any type of program or perform any procedure that may facilitate the entry of malicious and/or unwanted code capable of creating vulnerabilities in the production

environment or placing at risk the security of data stored in operating systems used by ZOOMHOLDING.

5.2 Software and hardware may not be installed on the corporate network without permission from the Information Technology Team. All updates and security patches for the operating system or applications may only be carried out after due validation in the respective testing environment and after being made available by the manufacturer or supplier.

5.3 Systems and computers must have antivirus software versions installed, activated, and permanently updated. Upon the slightest suspicion of a virus or antivirus uninstallation, the employee must report the suspicion to the Information Technology Team and must not perform any procedure.

5.4 The electronic mail of any ZOOMHOLDING domain address may only be used for purposes strictly related to the employee's activities, and the following is **strictly prohibited**:

a) sending messages to multiple recipients who have no connection with one another or with the subject matter of the message;

b) disclosing unauthorized information or screenshots of systems, documents, and similar materials, without the express and formal authorization granted by the data subject;

c) accessing links or opening files sent by e-mail that contain electronic threats such as spam, mail bombing, computer viruses, or that contain messages clearly unrelated to the corporate environment, or files with executable code, including .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf, or any other extension that may pose a risk to information security.

5.5 Any information accessed, transmitted, received, or produced on ZOOMHOLDING's internet network is subject to disclosure, control, monitoring, and audit. Any attempt to change the security parameters established by the Information Technology Team shall be considered serious misconduct, subject to termination of the contractual relationship for cause.

5.6 Internet use must be primarily ethical and restricted to the performance of work-related duties. ZOOMHOLDING may block any file, website, domain, or application stored on its internet network in order to ensure compliance with its Information Security Policy.

5.7 News, update, government entity, and any other websites that enable professional updating, training, and development are freely accessible to employees.

5.8 The use of the internet to commit unlawful acts, including any act contrary to Law No. 13,709/2018 (LGPD), shall result in termination of the employment contract for cause, in addition to any applicable administrative and criminal measures, in which case ZOOMHOLDING shall actively cooperate with the competent authorities, including the ANPD (Brazilian National Data Protection Authority).

5.9 The use of USB flash drives is prohibited and may only occur upon authorization from the Information Technology Team, provided that the principles of Purpose Limitation, Adequacy, Necessity, and Security in the storage and transfer of the information recorded therein are duly demonstrated.

5.10 ZOOMHOLDING, as the owner of the equipment and holder of the license rights to the operating systems used for the collection, storage, and archiving of information, reserves the right to inspect them at any time, regardless of prior notice, in order to monitor and control the effectiveness of security mechanisms.

5.11 Under no circumstances shall any change to the configuration of the equipment's operating systems be permitted, especially those related to security and log generation, except in the event of a technical justification duly guided by the Information Technology Team.

VI – FINAL PROVISIONS:

6.1 This Privacy and Information Security Policy shall be reviewed periodically. ZOOMHOLDING reserves the right to amend it whenever necessary, without prior notice and regardless of consent.
6.2 In accordance with Article 48 of Law No. 13,709/2018, ZOOMHOLDING shall notify the Data Subject and the Brazilian National Data Protection Authority (ANPD) of the occurrence of any security incident that may result in relevant risk or damage to the Data Subject.
6.3 Any questions or requests for clarification regarding the application of this Policy may be sent to ZOOMHOLDING's Data Protection Officer:

RAFAEL PETRELLA
E-mail: rafael.petrella@zoomholding.com.br

Nilton Pedro da Silva Junior
Chairman of the Board of Directors / CEO

Cassiano Hilario Bernardo da Silva
Vice-Chair of the Board of Directors

Natasha Utescher
Member of the Board of Directors

Marcelo Silveira
Corporate Governance Director

Lisiane Paula Pelisser
Finance Director

Rafael de Souza Petrella
Innovation Director