INFORMATION SECURITY POLICY

RTERY PRODUÇÕES LTDA., a private legal entity enrolled with the Brazilian National Register of Legal Entities (CNPJ) under No. 13.532.541/0001-02, with registered office at Rua Conselheiro Olegário, No. 258, Vila Anastácio, São Paulo, State of São Paulo, ZIP Code 05093-040, herein represented in accordance with its Articles of Association by its managing partner, Ms. Carolina de Melo Barreto, hereinafter simply referred to as "**ARTERY**".

This **INFORMATION SECURITY POLICY** (the "Policy") of **ARTERY** shall be governed by the following provisions and by all other applicable laws and regulations:

PREAMBLE - INTRODUCTION TO THE INFORMATION SECURITY POLICY

ARTERY recognizes information security as an essential element in protecting its business, reputation and the information of its employees, clients, suppliers, service providers, business partners and other stakeholders.

Accordingly, this Information Security Policy establishes guidelines for the responsible, secure and appropriate use of information, systems, equipment and other technological resources made available by **ARTERY**, in alignment with the principles of ethics, integrity, transparency, responsibility and respect that guide the Company's activities.

The protection of information and data processed by **ARTERY** is the responsibility of all persons who, directly or indirectly, have access to its resources or information. Each Authorized User must comply with the provisions of this Policy, all other applicable internal rules and applicable laws and regulations.

To the extent applicable, this Policy forms an integral part of the relationships maintained by ARTERY with its employees, officers, shareholders, suppliers, service providers, business partners and other third parties acting on behalf of or for the benefit of the Company, without prejudice to the obligations set forth in specific agreements.

I - PURPOSE

1.1. The purpose of this Policy is to establish guidelines enabling all employees, officers, shareholders, business partners, suppliers, service providers and other third parties with access to **ARTERY**'s resources or information to comply with appropriate information security standards consistent with the Company's business needs and with the protection of its information, data, systems and other assets. To this end, this Policy addresses the following principles and objectives:

I - Provide guidance for the establishment of specific information security rules and procedures, as well as for the implementation of controls and processes necessary to ensure compliance therewith;

II - Provide all employees with guidance regarding the use of computing, telecommunications and IT infrastructure resources;

III - Integrity. Ensure that information remains in its original and accurate state while stored or transmitted, protecting it against unauthorized, intentional or accidental modification;

IV - Confidentiality. Ensure that information is accessible only to authorized persons;

V - Availability. Ensure that authorized users have access to information and related assets whenever necessary.

II - ABRANGÊNCIA

2.1. This Policy applies to all employees, officers, shareholders, interns, suppliers, service providers, business partners and other third parties that maintain a relationship with **ARTERY** and that, directly or indirectly, use, access or support the Company's systems, infrastructure, equipment, technological resources or information. For purposes of this Policy, all such persons shall be referred to as "Authorized Users" or "users," as applicable.

III - GUIDELINES FOR THE USE OF ELECTRONIC EQUIPMENT

3.1. Users should preferably use electronic equipment owned by **ARTERY** for professional activities.

3.2. The use of personal equipment on **ARTERY**'s internal network is subject to compliance with applicable security requirements.

3.3. In the event of any questions and/or issues relating to equipment, systems or internal software, users must immediately notify the Company's management. Failure to provide prompt notice may result in the user being held responsible for any incidents that could have been prevented through timely notification.

IV - RESPONSIBILITIES

4.1. Authorized Users shall have the following specific responsibilities:

I - Each Authorized User shall be responsible for any loss or damage suffered by such Authorized User or caused to **ARTERY** and/or third parties as a result of failure to comply with the guidelines and rules set forth herein. In the event of any damage resulting from misuse or negligence, the user shall bear the costs associated with repairing or restoring the equipment;

II - Maintain exemplary information security practices, periodically back up information using the infrastructure made available by **ARTERY**, refrain from sharing passwords, and refrain from disseminating inaccurate or unreliable news or information.

4.2. **ARTERY** and/or the relevant departments and processes shall have the following responsibilities:

I - Upon engagement and execution of individual employment agreements, service agreements or partnership agreements, inform employees and other applicable parties of their responsibility to comply with this Policy and **ARTERY**'s other policies;
II - Require employees to execute the applicable Confidentiality Agreement, comply with the established rules, and undertake to maintain the secrecy and confidentiality of all **ARTERY** information assets.

V - ENVIRONMENT MONITORING AND AUDITING

5.1. In order to ensure compliance with the rules established in this Policy, **ARTERY** may:

I - Implement monitoring systems on workstations, third-party platforms, servers, corporate e-mail accounts, internet connections, mobile or wireless devices and other network components. Information generated by such systems may be used to identify users and their respective access activities, as well as the materials accessed or handled;
II - Disclose information obtained through monitoring and auditing systems where required by court order or requested by a manager or other senior officer;
III - Conduct physical inspections, at any time, of equipment owned by **ARTERY**;
IV - Install preventive and detective security systems and controls to ensure the security of information and access perimeters.

VI - USE OF CORPORATE E-MAIL SERVICES

6.1. The purpose of this section is to inform Authorized Users of the permitted and prohibited activities relating to the use of **ARTERY**'s corporate e-mail services.

6.2. Authorized Users are prohibited from using **ARTERY**'s corporate e-mail services to:

I - Send unsolicited messages to multiple recipients, except where related to legitimate **ARTERY** business purposes;
II - Send e-mail messages using a department's e-mail address, another person's username or any e-mail address that the user is not authorized to use;

III - Send any electronic message that may expose the sender and/or **ARTERY** to civil or criminal liability;

IV - Disclose unauthorized information or screenshots of systems, documents or similar materials without the express and formal authorization of the owner of the relevant information asset;

V - Falsify addressing information or alter message headers in order to conceal the identity of senders and/or recipients for the purpose of avoiding applicable penalties;

VI - Create, transmit or distribute any message containing any act or instruction that conflicts with or is contrary to **ARTERY**'s interests;

VII - Transmit or contain electronic threats, including spam, phishing attempts or computer viruses;

VIII - Contain files with executable code (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) or any other file extension that may pose a security risk;

IX - Seek to obtain unauthorized access to another computer, server, system or network device;

X - Seek to disrupt any service, server or computer network by any unlawful or unauthorized means;

XI - Seek to circumvent any security system;

XII - Seek to secretly monitor or harass another user;

XIII - Seek to access confidential information without the express authorization of its owner;

XIV - Seek to improperly access information in a manner that may cause harm to any person;

XV - Include encrypted or otherwise concealed images;

XVI - Contain attachments exceeding 20 MB for outgoing messages, whether internal or external, or 20 MB for incoming external messages;

XVII - Contain content deemed inappropriate, obscene or unlawful;

XVIII - Contain defamatory, degrading, offensive, violent, threatening, pornographic or similar content;

XIX - Contain discriminatory harassment based on sex, race, physical or mental disability, or any other protected characteristic;

XX - Be intended for local or national political purposes, including political advertising;

XXI - Include copyrighted material without the permission of the applicable copyright holder.

VII - <u>USE OF INTERNET SERVICES</u>

7.1. Any information accessed, transmitted, received or created through the internet may be subject to disclosure and auditing. Accordingly, and in full compliance with applicable law, **ARTERY** reserves the right to monitor and record all internet access activities.

7.2. The equipment, technology and services provided for internet access are the property of the Company. **ARTERY** may review and, where necessary, block any file, website, e-mail, domain or application stored on or accessed through the network or internet, whether stored on a local drive, workstation or private network area, in order to ensure compliance with this Information Security Policy.

7.3. By monitoring its internal network, **ARTERY** seeks to ensure the integrity of its data and software. Any attempt by an Authorized User to modify security settings without the appropriate credentials and authorization shall be deemed inappropriate, and the associated risks shall be communicated to such Authorized User. The use of any resource for unlawful activities may result in administrative measures and civil and criminal penalties. In such cases, the Company shall actively cooperate with the competent authorities.

7.4. As **ARTERY** considers it important for its Authorized Users to remain well informed, access to news websites, service websites and similar resources is permitted, provided that such use does not compromise network bandwidth during regular business hours, interfere with the proper performance of work activities or create conflicts of interest with **ARTERY**'s business objectives.

7.5. Only employees duly authorized to speak on behalf of **ARTERY** may communicate with the media, whether by e-mail, online interview, podcast, written document or any other means.

7.6. Only employees authorized by **ARTERY** may copy, capture, print or send screenshots to third parties and must comply with the Company's internal rules regarding the use of images, applicable copyright laws, constitutional protections relating to image rights and all other applicable legal provisions.

7.7. The improper disclosure and/or sharing of information relating to **ARTERY**'s departments or business areas through discussion lists, websites, social networking communities, chat rooms, instant messaging services or any other similar technology available or subsequently developed on the internet is prohibited.

7.8. The unauthorized use, installation, copying or distribution over the internet of software protected by copyright, trademark or patent rights is expressly prohibited. Any unauthorized software that is downloaded shall be removed by **ARTERY**.

7.9. Under no circumstances may employees use **ARTERY**'s resources to download or distribute pirated software or data, which constitutes unlawful conduct under applicable Brazilian law.

7.10. Materials of a sexual nature may not be displayed, stored, distributed, edited, printed or recorded using any **ARTERY** resource.

7.11. Access to peer-to-peer software and services (such as Kazaa, BitTorrent and similar services) is prohibited. Streaming services and instant messaging platforms (such as online radio, broadcast channels, WhatsApp, X and similar services), however, are permitted.

VIII - AUTHORIZED USER IDENTIFICATION

8.1. Identification devices and passwords are personal and are intended to protect the identity of each Authorized User by preventing improper access to and unauthorized use of **ARTERY**'s systems, information and technological resources.

8.2. The improper use, sharing or disclosure of third-party identification devices, credentials or passwords is expressly prohibited and may subject the responsible person to the applicable administrative, contractual and legal measures.

8.3. These rules are intended to establish accountability criteria for the use of identification devices and shall apply to all employees.

8.4. Accordingly, personal identification devices may not, under any circumstances, be shared with any other person.

8.5. Where a login credential is shared by more than one employee, the users of such credential shall be responsible before **ARTERY** and under applicable civil and criminal law for its use.

8.6. Sharing login credentials for system administration functions is prohibited, as is the exchange of equipment between users without proper authorization.

8.7. Each user is responsible for memorizing their own password and for protecting and safeguarding any identification devices assigned to them.

8.8. Passwords must not be written down or stored in electronic files (such as Word, Excel or similar files) in human-readable, unencrypted form. Passwords must not be based on personal information, such as the user's name, family members' names, date of birth, address, vehicle license plate, Company name or department name, nor may they consist of obvious keyboard or numerical combinations, such as "abcdefgh," "87654321" or similar combinations.

8.9. If an employee forgets their password, they must formally request that it be changed or contact the responsible technical department to have a new password created.

8.10. Any matters not expressly addressed in this section shall be handled in accordance with the most restrictive applicable security standard.

ARTERY™

IX - COMPUTERS, MOBILE DEVICES AND TECHNOLOGICAL RESOURCES

9.1. All equipment made available to employees is the property of **ARTERY**. Each employee is responsible for properly using and handling such equipment for activities related to the Company's business and for complying with the recommendations set forth in the operating procedures provided by the responsible management departments.

9.2. All operating system and application security updates and patches shall be performed by the responsible IT technical personnel after they are made available by the applicable manufacturer or provider.

9.3. The following uses of **ARTERY** computers and technological resources are prohibited:

I - Attempting to obtain or obtaining unauthorized access to another computer, server, system or network;
II - Circumventing any security system;
III - Accessing confidential information without the express authorization of its owner;
IV - Secretly monitoring another person through electronic devices or software, including, for example, packet analyzers (sniffers);
V - Disrupting any service, server or computer network through any unlawful or unauthorized method;
VI - Using any technological resource to commit or assist in acts involving infringement, sexual harassment, disruption, manipulation or infringement of copyrights or other intellectual property rights without proper authorization from the rights holder;
VII - Hosting pornographic, racist or any other material that violates applicable law, public morality, generally accepted standards of conduct or public order;
VIII - Using pirated software, which constitutes unlawful conduct under applicable Brazilian law.

9.4. For purposes of this Policy, a "mobile device" means any electronic equipment with mobile functionality owned by **ARTERY**, including laptops, smartphones, external hard drives and USB flash drives.

9.5. These rules are intended to establish criteria regarding the handling, prevention of risks and accountability associated with the use of mobile devices and shall apply to all employees who use such equipment.

9.6. As the owner of the equipment provided to employees, **ARTERY** reserves the right to inspect such equipment at any time when necessary for security maintenance purposes.

9.7. Employees therefore undertake not to use, reveal or disclose to third parties, in any manner whatsoever, directly or indirectly, for their own benefit or for the benefit of any third party, any information, whether confidential or otherwise, of which they become aware as a result of their duties, including after termination of their contractual relationship with **ARTERY**.

9.8. Employees are responsible for ensuring that they do not retain or use any programs and/or applications that have not been installed or authorized by **ARTERY**.

9.9. Unauthorized reproduction of software installed on mobile devices provided by the Company shall constitute misuse of the equipment and an infringement of the software manufacturer's copyrights.

9.10. In the event of theft or robbery of a mobile device provided by **ARTERY**, the employee is responsible for immediately notifying **ARTERY**'s officers. The employee must also contact the appropriate law enforcement authorities and file a police report as soon as possible.

9.11. Each Authorized User acknowledges that the misuse of a mobile device entails the assumption of all risks arising from such misuse and that the user shall be solely responsible for any resulting direct or indirect damages.

X - INFORMATION CLASSIFICATION

10.1. Information classification is an essential process for the security, management and protection of information and data processed by **ARTERY**.

10.2. Accordingly, sensitive or confidential information, including personal data and strategic, commercial, financial, operational or other information whose disclosure, alteration, loss or unauthorized access could cause harm to **ARTERY** or third parties, must be subject to strict protection measures. Such information must be securely stored, processed and transmitted in order to minimize the risks of data breaches, loss or cyberattacks, in compliance with the Brazilian General Data Protection Law (Law No. 13,709 of August 14, 2018 – "LGPD").

XI - PENALTIES

11.1. If any failure to comply with the guidelines established herein or any conduct prohibited under this Policy is identified (each, a "Violation"), appropriate measures shall be adopted based on the seriousness of the conduct, the extent of the damage caused, the degree of responsibility of the person involved, whether the conduct was intentional or negligent, any recurrence, and any other relevant circumstances of the particular case.

11.2. Suspected Violations of this Policy may be subject to review and investigation by the persons designated by **ARTERY**, taking into account, where applicable, principles of confidentiality, impartiality, proportionality and respect for the persons involved.

11.3. Depending on the nature of the relationship maintained with **ARTERY** and the seriousness of the matter, Violations may result in the cumulative or non-cumulative application of appropriate measures, including:

I - Formal warning;
II - Suspension or restriction of access to systems, equipment, information or technological resources;
III - Retrieval or replacement of equipment made available by **ARTERY**;
IV - Adoption of corrective measures to contain the incident and prevent recurrence;
V - Contractual, civil and/or criminal liability, where applicable; and
VI - Termination of the contractual or professional relationship, where applicable.

11.4. Each Authorized User shall be responsible for the proper care and maintenance of any **ARTERY**-owned equipment in their possession or use. Any damage to, misplacement and/or total loss of such equipment may result in the responsible person being held liable for losses demonstrably caused to ARTERY and/or third parties, subject to the applicable contractual arrangements and applicable law.

XII - VALIDITY OF THE POLICY

12.1. This Policy shall be made available to all Authorized Users subject to its provisions in a clear, accessible and up-to-date manner.

12.2. This Policy shall become effective upon its approval and may be reviewed and updated whenever necessary, particularly in light of changes to processes, technological resources, information security risks, applicable laws or any other circumstances warranting its revision.

12.3. **ARTERY** shall be responsible for communicating any updates or new versions of this Policy to Authorized Users and for making the document available for their acknowledgment and consultation.

12.4. The most recent version of this Policy supersedes all previous versions and shall become effective as of the date of its approval.

Last updated: September 16, 2026.