INFORMATION SECURITY POLICY

7COMm Group is a Brazilian technology company specializing in software analysis and development services, digital solutions, cybersecurity, vulnerability testing, software licensing, business intelligence, and artificial intelligence.

In its activities, 7COMm Group recognizes the critical importance of information and technology assets for its operations and for the trust of its clients, partners, and employees. As part of its commitment to ensuring the protection of information assets, it has established this Information Security Policy. This policy applies to all directors, administrators, employees, interns, trainees, service providers, and partners who use the processing environment or access Group information.

This commitment to protecting information assets owned by us and those under our custody is reflected in a robust Information Security and Privacy Management System (ISPMS), in compliance with market best practices, ISO/IEC 27001, ISO/IEC 27701 standards, and the General Data Protection Law (LGPD).

Our main objectives are:

1. **Ensure Confidentiality:** Guarantee that sensitive information and data are accessible only to authorized individuals, entities, or processes, preventing unauthorized disclosure or access.
2. **Ensure Integrity:** Maintain the accuracy and completeness of information and assets, preventing unauthorized or improper modifications. Any changes must be carried out exclusively by authorized individuals and in a standardized manner.
3. **Ensure Availability:** Ensure that information assets and essential services are accessible and usable by authorized individuals whenever needed, in accordance with policies and terms of use.
4. **Ensure Authenticity:** Confirm the origin and reliability of information, ensuring it comes from legitimate sources and has not been tampered with.
5. **Promote Continuous Improvement:** Continuously work to maintain and improve the security, efficiency, and effectiveness of the ISPMS, keeping our systems updated and protected against emerging threats.
6. **Maintain Compliance:** Ensure adherence to applicable data protection and privacy laws, regulations, and standards.

Main Guidelines and Responsibilities:

- **Shared Responsibility:** Every individual who interacts with 7COMm's assets and information is responsible for their protection and safeguarding and must treat information as a critical business resource.

- **Incident Reporting:** Any breach or suspected breach of information security must be immediately reported to management and leadership through available channels.
- **Access Management:** Logical access to 7COMm's internal network and systems is controlled through user credentials and passwords, which are personal and non-transferable. Access is granted based on the principle of least privilege.
- **Human Resources:** Information security is addressed throughout the employee lifecycle, from hiring (including background checks and confidentiality agreements) to termination (including access revocation and asset return).
- **Use of Equipment and Software:** The use of USB drives or non-corporate cloud storage services is prohibited. Installation of illegal or unauthorized software is strictly forbidden.
- **Internet and Email Usage:** The use of internet and corporate email is intended for professional purposes and is monitored to ensure compliance with policies and prevent threats. Accessing inappropriate content or disclosing confidential information is prohibited.
- **Data Sharing:** Sharing folders on local computers is prohibited; all data must be stored on network servers with controlled access.
- **Monitoring:** 7COMm Group environments are monitored by video cameras to ensure the safety of assets and individuals, with image processing in compliance with LGPD.
- **Sanctions:** Non-compliance with this policy constitutes a serious offense and may result in administrative sanctions (warning, suspension) or legal actions (termination of employment, civil/criminal proceedings), depending on severity and damage caused.

This policy is reviewed and updated periodically every 12 months or earlier if necessary.