São Paulo, August 28, 2026.

INFORMATION SECURITY POLICY – 7COMm

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

In its activities, Grupo 7COMm recognizes the criticality of information and technology assets for its operations and for the trust of its clients, partners, and employees and, as part of its commitment to ensuring the protection of information assets, has established this Information Security Policy. This policy applies to all directors, officers, employees, interns, apprentices, service providers, and partners who use the processing environment or access the Group's information.

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

Our main objectives are:

1. **Ensure Confidentiality:** Ensure that sensitive information and data are accessible only by authorized individuals, entities, or processes, preventing improper disclosure or access.
2. **Ensure Integrity:** Maintain the accuracy and completeness of information and assets, preventing unauthorized or improper modifications. Any change must be made exclusively by authorized persons and in a standardized manner.
3. **Ensure Availability:** Ensure that information assets and essential services are accessible and usable by authorized persons whenever necessary, in accordance with policies and terms of use.
4. **Ensure Authenticity:** Confirm the origin and veracity of information, ensuring that it comes from legitimate sources and has not been forged.
5. **Promote Continuous Improvement:** Conduct continuous efforts to maintain and improve the security, efficiency, and effectiveness of the SGSPI, keeping our systems up to date and protected against emerging threats.
6. **Maintain Compliance:** Ensure compliance with relevant Data Protection and Privacy laws, regulations, and standards.

Main Guidelines and Responsibilities:

- **Everyone's Responsibility:** Each individual who interacts with 7COMm's assets and information is responsible for their protection and safeguarding, and must treat information as a critical resource for the business
- **Incident Communication:** Any violation or suspected violation of information security must be immediately communicated to management and leadership through the available channels.
- **Access Management:** Logical access to 7COMm's internal network and systems is controlled by 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 life cycle, from hiring (with background checks and confidentiality agreements) to termination (with revocation of access and return of assets).
- **Use of Equipment and Software:** The use of flash drives or non-corporate cloud storage services is prohibited. The installation of illegal or unauthorized software is strictly prohibited
- **Use of Internet and Email:** The use of the internet and corporate email is intended for professional purposes and is monitored to ensure compliance with policies and to prevent threats. Access to inappropriate content or disclosure of 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:** Grupo 7COMm's environments are monitored by video cameras for the security of property and people, with the processing of images in compliance with the LGPD.
- **Sanctions:** Non-compliance with this Policy constitutes serious misconduct and may result in administrative sanctions (warning, suspension) or legal sanctions (termination of the employment contract, civil/criminal proceedings), depending on the severity and the damage caused.

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