VULTUS	Main process	Information Security
	Process title	Information Security Management System (SGSI)
	Department / Owner	Information Security
	Revision code	007.06

Our Commitment to Security and Privacy

At Vultus, security and privacy are more than part of our operations: they are the pillars supporting our entire digital ecosystem. We know the trust of our clients, partners, and employees is essential, so we handle information protection with the highest level of responsibility and transparency.

Foundations and International Standards

Our internal information security and privacy policy follows established principles of confidentiality, integrity, availability, and accountability in data processing. It incorporates controls and practices based on ISO/IEC 27001:2022 and ISO/IEC 27701:2019, globally recognized standards for security and privacy management. These controls include, among others:

- Encryption and protection of data at rest and in transit;
- Security incident management and event response;
- Access controls and digital identity;
- Cloud environment security;
- Vendor and third-party management;
- Ongoing training and awareness programs;
- Continuous improvement and periodic review of policies and procedures.

Continuous Protection and Governance

Our Information Security and Privacy Management System (SGSPI) is structured to continuously identify, assess, and address risks, ensuring protection of the information entrusted to us. This governance is supported by auditing, monitoring, and improvement processes that ensure compliance and the effectiveness of implemented controls.

Responsible Partnerships and a Secure Value Chain

Vultus maintains relationships with vendors and partners who share our security principles. All are assessed against compliance and data protection criteria so that the same security standard extends throughout the value chain.

Transparency and Compliance

We comply with Brazil's General Data Protection Law (LGPD) and other applicable regulations, maintaining an ongoing compliance program. We value transparency in our practices and are always available to demonstrate how we protect and process data ethically, securely, and responsibly.

Reporting Channel

Suspected information security violations or unethical conduct may be reported confidentially, with protection against retaliation, at denuncias@vultuscyber.com.br.

VULTUS		
	Main process	Information Security
	Process title	Information Security Management System (SGSI)
	Department / Owner	Information Security
	Revision code	007.06

A Lasting Commitment to Excellence

Security and privacy are part of Vultus's identity. We maintain an ongoing commitment to innovation, improvement, and compliance, evolving our practices to ensure our clients and partners always have a secure, reliable, and resilient digital environment.

Revision History

Revision	Date	Revised content
014.01_CRC	Oct 16, 2023	Creation of Vultus Cybersecurity's Public ISMS Policy, based on industry best practices and aligned with organizational strategy.
014.02_CRC	Oct 17, 2023	Review of section 4.1.3 and removal of section 7 (Approvals) from SGSIP as a security measure for a public document.
014.03_CRC	Oct 20, 2023	Updated the header with the document version description.
014.04_CRC	Oct 9, 2024	Review of the logo, organization name, and layout.
007.05	Oct 29, 2025	General policy review, filename, and version naming.
007.06	Oct 24, 2026	Management system acronym corrected to SGSPI and LGPD compliance wording adjusted. Added the reporting channel. Standardized layout, owners, and publication through resources provided by Vultus. Corrected the reporting channel (denuncias@) and standardized the VULTUS Cybersecurity name (October 29, 2026).

Approvals

Owner	Date	Signature
Executive Leadership	Oct 30, 2026	Alexandre Brum
Information Security	Oct 30, 2026	Caio Oliveira