



Information Security and Data Protection Policy

The Management of TANCAMED, S.A., recognises information as a strategic asset for the provision of its chemical and food transport services, and undertakes to protect it from internal and external threats, ensuring its confidentiality, integrity, availability, authenticity and traceability. This Policy is established in compliance with Regulation (EU) 2016/679 (GDPR), Spanish Organic Law 3/2018 on the Protection of Personal Data and the Safeguarding of Digital Rights (LOPDGDD), the requirements of the SQAS scheme and the principles of the ISO/IEC 27001 standard.

This Policy applies to all information processed by TANCAMED, S.A., in any medium (digital, physical or oral), to its information systems, networks, devices and services, and to all permanent and temporary personnel, subcontractors, suppliers and interested parties with access to such information.

Management hereby declares and undertakes to:

- Confidentiality: ensuring that information is only accessible to those duly authorised, particularly customer, product, operational, personal and commercial data.
- Integrity: ensuring the accuracy and completeness of information and of its processing methods.
- Availability: ensuring access to information and related resources whenever required by authorised users, through backups, business continuity plans and proactive maintenance.
- Compliance with the GDPR and the LOPDGDD: lawful, fair and transparent processing of personal data, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.
- Compliance with data subjects' rights (access, rectification, erasure, objection, restriction, portability and the right not to be subject to automated decisions).
- Performance of Data Protection Impact Assessments (DPIA) where appropriate, and maintenance of the Record of Processing Activities.
- Annual information-security risk assessment, addressing cyber threats (malware, phishing, ransomware, denial-of-service attacks), security of mobile devices, EDI exchanges and cloud services, and application of proportionate technical and organisational measures.
- Up-to-date inventory of information assets (hardware, software and data), with identification of owner, custodian and criticality level.
- Proactive maintenance programme for IT assets, in accordance with manufacturers' recommendations.
- Annual audit of the information system by a person or entity independent of system development and operation.
- Communication to employees and subcontractors of threats and changes in the risk level, and of the response measures.

- Incident response procedure for security incidents and personal data breaches, including notification to the Spanish Data Protection Agency (AEPD) within 72 hours and to data subjects where applicable.
- Periodic training and awareness of personnel in information security, data protection and cybersecurity.
- Application of the privacy-by-design and privacy-by-default principles in any new system, process or service.
- Selection and oversight of data processors through contracts compliant with Article 28 GDPR, and verification of their technical and organisational safeguards.

This Policy is disseminated to all personnel upon joining the Company and through internal communication channels. It will be reviewed at least once a year, and whenever significant changes occur in the organisation, in the services provided, in the regulatory framework or in the threat landscape.

Managing Director, Tancomed S.A.
Approval date: 12.01.2026