

Information and Privacy Security Policy.

CSi palletising provides fully integrated material handling systems throughout the world. The core activities include design, development, sales, assembly, installation and maintenance of conveyor systems and palletising installations.

This policy applies to all employees and contractors of CSi industries BV at our location in Raamsdonksveer in The Netherlands and all our activities carried out at customer locations under the responsibility of CSi palletising.

Purpose

CSi is committed to protecting the information of our customers, employees and business partners. We protect all information that we collect, create, exchange and store. Our goal is to maintain the confidentiality, integrity and availability of this information.

Our commitments

To protect information and personal data, CSi will:

- keep confidential information secure and only allow access to authorised persons
- maintain the accuracy, completeness and availability of information and information systems
- protect information systems against unauthorised access, misuse and other security risks
- assess information security and privacy risks and implement appropriate measures
- train employees to store and exchange confidential and personal data correctly, recognise suspicious activities and report incidents
- classify and handle information according to its sensitivity, business value, legal requirements and importance to operations
- assess relevant suppliers for information security and privacy risks
- identify, report, investigate the root cause and respond to security and privacy incidents with remedial actions, and use the lessons learned to prevent them from happening again
- maintain and test a Business Continuity Plan to support the continuity of our services
- comply with applicable information security and privacy laws, including the General Data Protection Regulation (GDPR)
- protect physical access to our offices and facilities
- continuously improve the ISMS.

Information Security Management System (ISMS)

CSi maintains an Information Security Management System, or ISMS, in accordance with ISO/IEC 27001:2022. We use the ISMS to manage information security and privacy risks, document our controls and demonstrate compliance with applicable requirements.

We regularly evaluate our controls through risk assessments, penetration tests, internal and external audits and management reviews. We record necessary improvements in an action plan, monitor their implementation and use the results to support the continuous improvement of our information security and privacy management.

CSi sets measurable information security and privacy objectives. The progress on these objectives are monitored throughout the year and reviewed during the annual management review.

Security throughout the lifecycle

CSi applies a risk-based approach to information security and privacy. Security responsibilities are assigned and communicated, and information is classified and protected according to its sensitivity.

CSi protects its IT systems, operational technology and remote connections. Where applicable, cybersecurity is considered during the design, development, testing, delivery, maintenance and end-of-life of machines, software, firmware and 3rd party products.

CSi manages access rights, vulnerabilities, security updates, backups, recovery arrangements and relevant supplier risks. These measures are regularly reviewed to support the continuous improvement of the ISMS.

Responsibility and review

The CSi Management Team is ultimately responsible for this policy and ensures that information security responsibilities are assigned, documented and communicated. CSi has designated a Chief Information Security Officer (CISO) to oversee and coordinate information and privacy security across the organization and provides independent advice to the Management Team. All employees and relevant external parties are responsible for complying with the security requirements that apply to their activities.

CSi reviews this policy and the ISMS regularly and whenever significant changes occur. Based on these reviews, policies, procedures and security measures are updated where necessary. A review may be prompted by:

- organisational changes
- new or changed legal requirements
- changes in information security risks
- findings from audits
- significant security or privacy incidents.

Protecting information is a shared responsibility and an essential part of how we work at CSi.

Approved on 24th of September 2026,

R. van Dorst
General Managing Director