HOYER GROUP

REVIEW

Information Security Report 2026

WHEN IT MATTERS

Ladies and Gentlemen,
Friends of our Company,

As a family business, sustainability, safety, and security remain the guiding principles of the HOYER Group. These values shape our decisions and actions, anchoring us as we continue to innovate and lead in logistics. In 2026, digital transformation is accelerating our ability to deliver efficient, customer-focused solutions. With this progress comes a heightened responsibility to safeguard our digital information and business processes. Information security is not just a technical requirement – it is a strategic imperative for our competitiveness and reputation. The risks posed by cyberattacks are evolving rapidly, demanding vigilance and resilience. Our mission is clear: to protect our business, our clients, and our partners. Our Chief Information Security Officer, together with the Information Security and Governance, Risk and Compliance team, ensure that robust governance, policies, and technical capabilities are in place to manage these risks. This commitment is embedded within our Corporate Center IT Services.

We strive to anticipate tomorrow's challenges today. As a global leader in liquid goods logistics, HOYER stands for quality, sustainability, and trusted information security. Our customers and partners rely on us for secure, reliable service – and we are dedicated to meeting that trust every day.

With warmest regards from Hamburg,

Björn Schniederkötter
Chief Executive Officer HOYER Group

CERTIFIED QUALITY

Information Security Report 2026

The HOYER Group has a long-standing and intense focus on information security, safeguarding a sophisticated and interconnected IT system landscape. This report is intended to transparently present our security goals and achievements to our business partners.

Objectives of Information Security Management

The HOYER Group has set itself the goal of comprehensive information security management to protect its data and IT assets. Systems failure avoidance and the protection of information about employees and business partners are a top priority in the risk management of the Executive Board. Information security is taken into account from the very start of discussing new opportunities.

The constant growth in the IT connectivity of worldwide business, in parallel with the ongoing increasing complexity of information technology, creates a bigger target for cybercrime.

HOYER therefore pursues the following goals with its information security strategy:

- Maximization of business continuity
- Prevention and minimization of the effects of security incidents
- Limiting the risks from cybercrime

The HOYER Group has therefore implemented an Information Security Management System (ISMS), which provides comprehensive, far-reaching protection for IT assets and data. The HOYER Group Information Security Management System is based on ISO/IEC 27001:2022 and is designed to ensure the confidentiality, integrity and availability of our business information.

SCOPE

Provision and operation of central IT infrastructures and business applications for the transport and logistics management processes of the HOYER Group. Relevant cloud applications, in-house software development, the central data center and the provision of IT security are included.

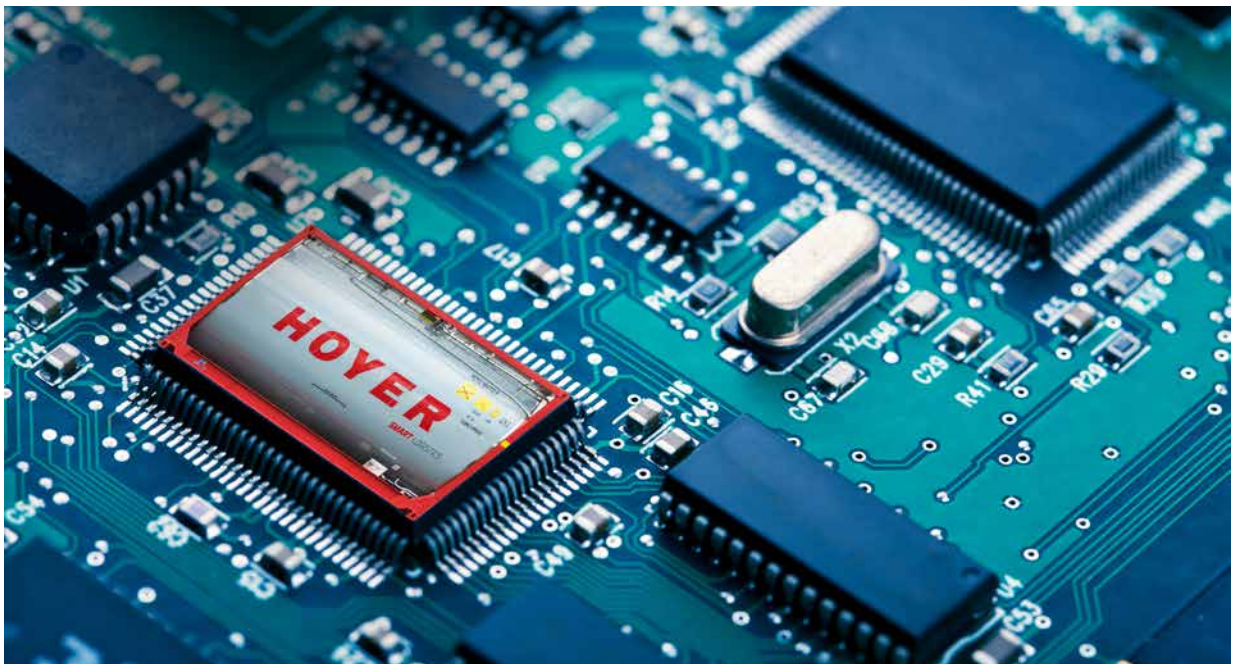
Technical implementation

To protect information assets, we take a multi-layered approach to building information security controls into every layer of technology, including data, endpoints and applications. This provides robust end-to-end protection, while at the same time offering numerous ways to identify, protect, detect, respond to and recover from cyber threats.

A special focus is placed on vulnerability management, security automation and the adoption of multi-factor authentication (MFA) across all systems.

Employee awareness and responsibility

Each employee is responsible for ensuring that the information security and procedures are implemented. Every new employee receives the information security guidelines and is trained on these important matters by his or her supervisor. In addition, all employees complete regular, mandatory online training courses on information security. The e-learning modules for information security teach all employees the behavior rules for handling data and IT assets, traced by our gamified training platform. On top of our trainings and policies we do raise awareness by our advanced phishing campaigns.



Security governance and control

The effectiveness of the Information Security Management System is reviewed annually by independent auditors and certification bodies. Contact with supervisory authorities is maintained by the Corporate IT management. There is close cooperation with our partners and suppliers in the area of information security and cyber defense. A penetration test is conducted at least annually, and the HOYER attack surface is monitored daily. To ensure 24/7 detect and respond procedures, we have contracted with one of our security partners to handle the security monitoring and immediate response.

Stakeholder involvement helps to ensure that we apply the most up-to-date information security approaches and techniques. HOYER has established a dedicated IT security team to actively manage customer requests, legislation, and technologies with the support of our partners and suppliers. Moreover, HOYER follows the principle of least privilege access for all its employees.

Information Security Management

At HOYER, the Chief Information Security Officer (CISO) serves as the principal authority for information security, directing the development and implementation of a comprehensive security strategy. The CISO oversees the maintenance of robust protective measures across the Group, ensuring the confidentiality, integrity, and availability of all business and customer information assets.

Employees are provided with clear and accessible channels to report security incidents via the central service desk. Upon notification, each incident is promptly assessed and managed by the IT Security team, in accordance with established protocols. HOYER maintains a rigorously defined and periodically tested emergency response plan, complemented by a Business Continuity Management Policy that delineates procedures and safeguards to be enacted during cyber security incidents.

The governance framework and security management systems of HOYER are subject to formal bi-annual review by senior management. This process ensures that security policies and standards remain responsive to evolving business needs, regulatory requirements, and emerging threats. These policies embody the explicit commitment of the Executive Board to information security, further underscored by the certification of HOYER to the international ISO 27001:2022 standard for information security management.

The Information Security Policy framework articulates the organization's core principles and encompasses comprehensive policies and procedures, which are made readily accessible to all employees. Within individual business units, designated application managers and business owners are entrusted with the operational responsibility for ensuring ongoing compliance with established information security principles.

Key figures on information security

Key indicators for information security are reported to and reviewed by the CISO and reported to the senior leadership team every quarter.

Annex to certificate
Registration no.: 519033 ISMS22

HOYER GmbH Internationale Fachspedition

Wendenstraße 414-424
20537 Hamburg
Germany

Location

520964
HOYER Global Transport B.V.
Oude Maasweg 50
(Harbour Route Number 4048)
3197 KJ Botlek Rotterdam
Netherlands

This annex (
with the ab

CERTIFICATE

This is to certify that

HOYER GROUP

HOYER GmbH Internationale Fachspedition

Wendenstraße 414-424
20537 Hamburg
Germany

with the organizational units/sites as listed in the annex

has implemented and maintains an **Information Security Management System**.

Scope:
Provision and operation of central IT infrastructures and business applications for the transport and logistics management processes of HOYER Group. Relevant cloud applications, in-house software development, the central data center and the provision of IT security are included.

Statement of applicability: version 1.0 from 2025-09-24

Through an audit, documented in a report, it was verified that the management system fulfills the requirements of the following standard:

ISO / IEC 27001 : 2022

Certificate registration no.	519033 ISMS22
Valid from	2025-10-12
Valid until	2026-10-15
Date of certification	2025-10-12

DQS IS A MEMBER OF

DQS GmbH

Guido Eggers
Managing Director

Accredited Body: DQS GmbH, August-Schanz-Straße 21, 60433 Frankfurt am Main, Germany
The validity of the certification can only be verified by the QR-code.

1 / 2

HOYER GmbH Internationale Fachspedition and HOYER Global Transport B.V. are certified according to ISO/IEC 27001:2022 standards.

HOYER GmbH
Internationale Fachspedition

Head Office
Wendenstrasse 414–424
20537 Hamburg | Germany
Phone +49 40 21044 0 | Fax +49 40 21044 246

hoyer@hoyer-group.com
www.hoyer-group.com