HOYER GROUP

REVIEW

Information Security Report 2022

WHEN IT MATTERS

Ladies and Gentlemen,
Friends of our Company,

As a family business, sustainability, safety and security are core values for the HOYER Group. They provide orientation, are firmly anchored and determine our decisions and actions. Everything we do is based on these values.

Strategically, we see ourselves as a sustainable innovation and technology leader. In this context, digitalisation is an essential driver of our efficient and continuously optimised logistics solutions and thus of our corporate development. The responsible handling of digital information flows requires an extremely high focus on information security.

Digitalisation brings a myriad of opportunities for logistics companies, enabling HOYER to offer customer-focused data exchange services and streamlined business processes. In addition to data protection, information security is also in the business interests of the HOYER Group. Any failure, manipulation or unauthorised disclosure of business-critical information can lead to significant financial losses or damage to the Group's image.

The adequate security of business processes, IT, infrastructure and critical information is therefore a strategic factor for the competitiveness and continued existence of the company. However, cyberattacks on businesses are increasing in scale, speed and sophistication. These developments expose HOYER to information security risks. This report will explain to you how HOYER tackles the important topic of information security.

Our mission is to protect the business and our clients. Our Chief Information Security Officer (CISO), established in 2018, ensures that the appropriate governance framework, policies, processes and technical capability are in place to manage these risks. This function sits within our Corporate Center IT.

To already work today on tomorrow's solutions – that is our aspiration. As one of the world's leading logistics specialists for liquid goods handling and transport, we stand for quality-oriented sustainable action, including information security – and our customers and partners appreciate us for that.

With warmest regards from Hamburg.

Björn Schniederkötter
Chief Executive Officer HOYER Group

CERTIFIED QUALITY

Information Security Report 2022

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. The failure of systems 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:

- Maximisation of business continuity
- Prevention and minimisation 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 : 2017 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 HOYER Group. Relevant cloud applications, in-house software development, the central data centre and the provision of IT security are included. The quality management processes cover the centralised IT based in Hamburg and Rotterdam locations.

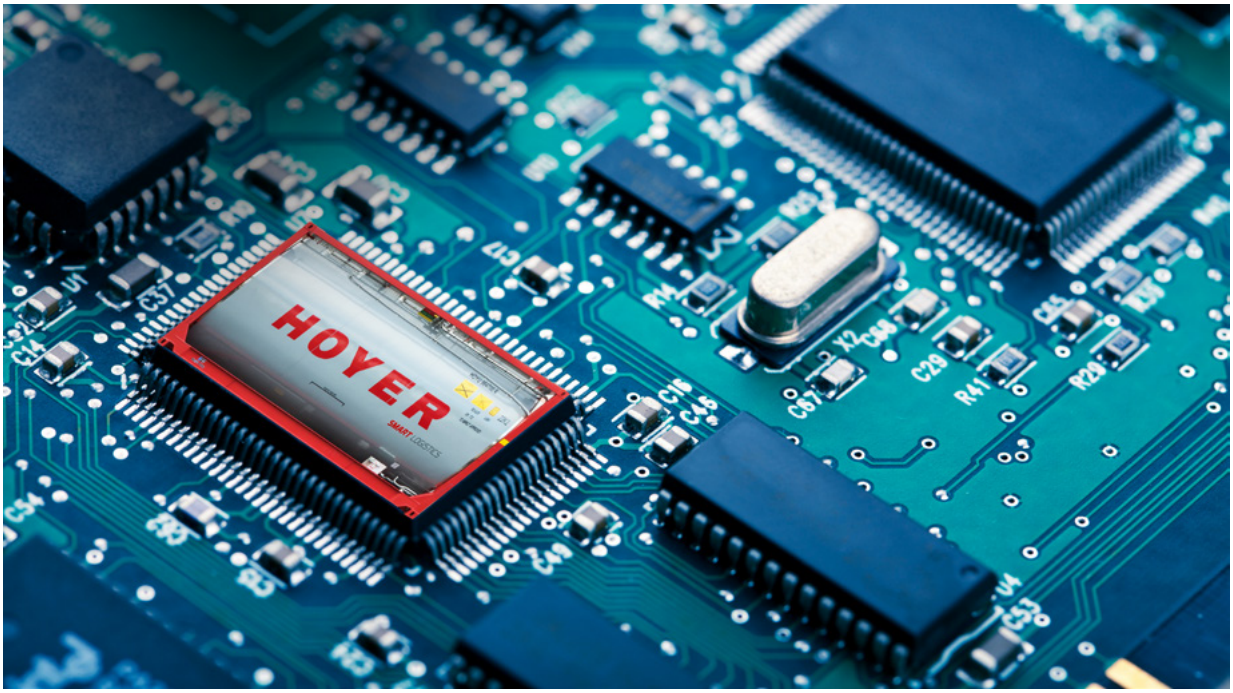
Technical implementation

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

A special focus is placed on patch management to keep vulnerabilities of operating systems, databases, networks and applications to an absolute minimum.

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 module for information security teaches all employees the behaviour rules for handling data and IT assets, traced by the global HR system for all HOYER employees. On top of our trainings and policies we do raise awareness by our bi-annual phishing campaign.



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 defence. A penetration test is conducted annually. To ensure 24-hour detect and respond procedures, we have contracted with one of our security partners to handle a significant portion of our security monitoring.

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 technologies, to coordinate the exchange of information and to develop relationships with our partners and suppliers. Moreover, HOYER is following the principle of least privilege for all its employees.

Information Security Management

As the central owner of information security for HOYER, our CISO is responsible for defining and implementing the information security strategy, maintaining an appropriate level of information security protection throughout the Group, and protecting the confidentiality, integrity and availability of business and customer information.

Every employee can report information security incidents via the central service desk. All security incidents are flagged as security-relevant and immediately evaluated and dealt with by the CISO and the IT Security team. An emergency plan for security incidents has been defined, introduced and tested. In addition, a Business Continuity Management Policy has been drafted on the measures and processes to be undertaken in the event of a cyber security incident.

Our governance framework and security management are reviewed annually by management to ensure that security policies and standards continue to reflect evolving business requirements, regulatory guidelines and emerging threats. The policies provide a formal statement of the Executive Board's commitment to ensuring the security of HOYER's information. To demonstrate its commitment, HOYER is certified to the international standard ISO 27001 for information security.

The Information Security Policy Framework, which contains the principles of information security as well as detailed information security policies and procedures, is available to all employees. Within the business units, Business Systems Managers and Business Owners of applications are responsible for the operational aspects of compliance with the information security principles.

Key figures on information security

Key indicators for information security are reported to and reviewed by the Director of Corporate IT and the Chief Financial Officer every month.

Annex to certificate
Registration No. 519033 ISMS17

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 (ed
with the above-

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. The quality management processes cover the locations Hamburg and Rotterdam.

Statement of applicability: Version 1.1 2020-09-02

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

ISO / IEC 27001 : 2013
Equivalent to: **DIN EN ISO / IEC 27001 : 2017**

Certificate registration no.	519033 ISMS17
Valid from	2020-10-16
Valid until	2023-10-15
Date of certification	2020-10-16

DQS GmbH

Markus Bleher
Managing Director

Accredited Body: DQS GmbH, August-Schanz-Straße 21, 60433 Frankfurt am Main, Germany

1 / 2

HOYER GmbH Internationale Fachspedition and HOYER Global Transport B.V. are certified according to ISO / IEC 27001 : 2017 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