CYBER SECURITY STATEMENT

The purpose of this Cyber Security Statement is to provide our clients, partners, suppliers and vendors, with information about our security practices and the way we manage information, data and cargo according to industry best practices and what can be expected.

Spliethoff Group

The Spliethoff Group is one of the largest shipping companies in the Netherlands. With over a century of maritime expertise, the Amsterdam-headquartered Group operates a large and modern fleet of more than 100 vessels ranging in size from 2,100 to 23,000 tons.
The Group has a broad portfolio of specialized services in the sectors dry cargo, breakbulk & project cargoes – Spliethoff –, project & heavy lifts – BigLift Shipping –, container & Ro-Ro cargo and door-to-door services – Transfennica & Transfennica Logistics –, shortsea – Wijnne Barends –, yacht transport – Sevenstar Yacht Transport – and RoRo- tonnage provider Bore.

Security Management

Safety and security are important to Spliethoff to protect its fleet, the cargo and the customer information that is managed by Spliethoff Group. Therefore, Spliethoff Group has chosen to use ISO 27000 as a guiding standard on how information security is managed. Furthermore, we follow and apply controls from the NIST Cybersecurity Framework, IMO regulations and industry guidelines, where applicable.

Information Security Policy

Spliethoff Group's security policies and procedures define how the different areas of information security are managed within the company and its subsidiaries.
The security policy is periodically reviewed, audited and updated where necessary. The policies and procedures cover a wide array of security topics, ranging from general standards – which all employees must read, understand and comply with, such as account, equipment, data and physical security – to more specialized security and maritime standards covering the internal systems and applications as well as maritime operational systems used on the vessels in the fleet.

Organisational Security

Information security roles and responsibilities are documented and defined so that our personnel and crew know their responsibilities. An appointed Cyber Security Group that manages information security, auditing and compliance and also defines the security controls for the protection of the Spliethoff Group infrastructure on land and sea. The Cyber Security Group is responsible for the managing of information security notifications from external parties, customers, vendors and suppliers, and distributes security alerts and advisory information to the organization on a regular basis after having assessed risk and impact as appropriate.

CYBER SECURITY STATEMENT

Personnel & Crew Security

All Spliethoff group employees are required to operate in line with the company policies, guidelines and procedures, including those covering confidentiality, integrity, availability, business ethics, appropriate usage, and applicable regulatory standards. All employees subscribe the company policies. Processes and procedures are implemented to manage employee's signing on and signing of from vessels to ensure proper management of users, credentials and authorizations. Employees are subject to security training as part of the signing on process. Security training is also provided for all office employees, as part of their familiarization training.

Asset Management

Spliethoff Group information systems, corporate business systems and maritime fleet operational systems are documented in a central register. These systems are managed according to our security policies and procedures. All Spliethoff personnel authorized to manage these assets are to comply with established policies, procedures and guidelines defined in the Spliethoff security management framework.

Access controls

Role-based access controls are implemented for access to information systems. Procedures are implemented to address employee's activities for signing on and off from vessels. All users are provided with unique account IDs. The password policy defines acceptable passwords for information systems, applications and databases. The password policy defines the use of complex passwords. Access to critical systems requires Multi-Factor Authentication (MFA, also known as 2FA).

Data Protection

Spliethoff information systems operate on the latest recommended encryption standards, ciphers and protocols to encrypt data at rest and traffic in transit. The data protection landscape is monitored to respond immediately to new cryptographic vulnerabilities and weaknesses when they are discovered. Guidelines and procedures are updated and implement when needed.

Physical security

Spliethoff has policies, procedures and the infrastructure to provide physical security of its data centers, offices and vessels. The security of the vessels is based upon the regulatory requirements outlined by IMO. The security controls implemented in offices and on vessels include the use of electronic access control systems, locks, burglary alarms, fire alarm and suppression systems and surveillance cameras.

CYBER SECURITY STATEMENT

Operations security

Spliethoff has documented operating procedures and responsibilities for all systems, applications and services in the environment. Change management process is implemented to document, approve and track all changes to the environment to ensure that changes work as expected and according to established policies, procedures and standards, and to ensure security and safety of operational systems.

Network Security

Spliethoff network infrastructure and servers are protected by high-availability firewalls and are configured for the detection and prevention of various network security threats. Firewalls are used to restrict access to systems and networks from external networks and between systems and networks internally. By default, all access is denied and only access based on business needs are allowed.

Software Development Lifecycle

Spliethoff follows a documented secure software development methodology designed to ensure that software is developed to be safe, secure, resilient and robust. Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing and product security assessments.

IT Supplier and Vendor Relationships

For its IT systems, software and networks and for the on-board systems with IT related components, Spliethoff uses partners, vendors and suppliers who operate with the same or similar values and requirements regarding security, data protection, safety, ethics, confidentiality, integrity and availability as Spliethoff does. Partners, vendors and suppliers that interact with Spliethoff IT systems, are screened and bound by appropriate security obligations to protect Spliethoff information, data and systems with special focus on proper management of customer data and critical operational systems. Occasionally, Spliethoff carry out audits to ensure the confidentiality, integrity and availability of the systems and data that third-party partners, vendors and suppliers manage.
For all on board systems connected to or using the IT infrastructure, access is limited to the cases where this access is necessary and restricted to the suppliers' systems only.

Incident management

Spliethoff has a documented incident response plan and procedures on how to manage security incidents. The incident response plan and procedures define the roles and responsibilities for incident management tasks, how incidents are managed, escalated and notified to relevant parties, including authorities.

Business Continuity and Disaster Recovery

In order to minimize system and service interruption due to hardware of software failures, natural disasters or other catastrophes, Spliethoff has implemented disaster recovery procedures for all critical business and operational systems.

CYBER SECURITY STATEMENT

Compliance

Spliethoff complies with the statutory and regulatory requirements and complies with the industry standards, when applicable. The system is regularly audited by third parties to ensure the policies, processes and procedures comply with established standards and requirements.

Contact

If you need more information on how Spliethoff manages cyber security, please contact our Cyber Security team using the following contact details: cybersecurity@spliethoff.com