FOLBB
virgin fiber cartonboard made personal

FOLBB – Group 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. This Cyber Security Statement applies to all IT and OT systems, networks, databases, applications, and all physical and digital data processing activities within FOLBB Group.

FOLBB Group

The FOLBB Group is a fiber carton board producer with locations in The Netherlands and Germany.

Security Management

Safety and security are important to FOLBB to the group our emplyees and the customer information that is managed by FOLBB Group. Furthermore, we follow and apply controls from the NIST Cybersecurity Framework and industry guidelines, where applicable.

Information Security Policy

FOLBB 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.

Organizational Security

Information security roles and responsibilities are documented and defined so that our employees know their responsibilities.

Employees Security

All FOLBB 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. Employees are subject to security training as part of the signing on process. Regular security awareness training for all employees, including phishing simulations, social engineering tests, and IT security updates.

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 and from outside the company requires Multi-Factor Authentication (MFA, also known as 2FA).

Data Protection

FOLBB 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

FOLBB has policies, procedures and the infrastructure to provide physical security of its data centers. 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.

Network Security

FOLBB 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. FOLBB implements network segmentation that ensures critical systems are isolated from less sensitive environments.

IT Supplier and Vendor Relationships

For its IT systems, software and networks and for the on-board systems with IT related components, FOLBB 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 FOLBB does. Partners, vendors and suppliers that interact with FOLBB IT systems, are screened and bound by appropriate security obligations to protect FOLBB information, data and systems with special focus on proper management of customer data and critical operational systems. Occasionally, FOLBB 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.

Compliance

FOLBB 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.