Cyber Security

The cyber security policy of TS-Shipping GmbH & Co. KG outlines our processes and provisions for preserving the security of our data and information technology (IT) infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, cyber threats and system malfunctions could result in penalties, cause great damage and may jeopardize our company's reputation.

For this reason, we have implemented cyber security procedures, which we have outlined in this policy.

Scope

This policy applies to all our employees ashore and crews onboard the fleet, service contractors and anyone who has permanent or temporary access to our systems and hardware.

Protection of Company Devices

- Enforce proper access control (onboard at the gangway as per SSP). Ensure that devices are not left exposed or unattended,
- Keep all devices password protected,
- Choose and upgrade a complete antivirus software. Install security updates of browsers and systems regularly or as soon as updates are available,
- Log into company accounts and systems through secure networks only.

We also advise our employees that it is strictly prohibited to access internal systems and accounts from other people's devices or lending their own devices to others. This includes, but is not limited to: onboard IT equipment incl. computers, navigationalequipment, planned maintenance systems, e-mail browser or other communication means.

Keep e-Mails Safe Ashore and Onboard

The company receives e-mails from all over the world. These e-mails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained,
- Be suspicious of clickbait titles (e.g. offering prizes, advice.),
- Check e-mail and names of people they received a message from to ensure they are legitimate,
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks).

Manage Passwords Properly

Password leaks are dangerous since they can compromise our infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advice our crews and employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays),
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done,
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of e-mail, and only if they personally recognize the person they are talking to,
- Change their passwords as per instructions from the company.

Transfer Data Securly

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask the company for help,
- Share confidential data over the company network/system and not over public Wi-Fi or private connection,
- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies,
- Report scams, privacy breaches and hacking attempts.

Our company needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees and crews to report perceived attacks, suspicious e-mails or phishing attempts as soon as possible as per our Safety Management System. Our company must investigate promptly, resolve the issue and send a companywide alert when necessary.

Take Cyber Security Seriously

- Turn off the screens and lock the devices when leaving the desks,
- Report stolen or damaged equipment as soon as possible to the DP/CSO,
- Change all account passwords at once when a device is stolen,
- Report a perceived threat or possible security weakness in company systems,
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment,
- Avoid accessing suspicious websites.

Everyone, from our customers to our employees, crews and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Haren, April 1st, 2021
Place and Date

Bölle, Alexander
Managing Director