MPC Container Ships ASA: Cyber Security Policy

Adopted by the Board of Directors
on June 24, 2024

1. INTRODUCTION

MPC Container Ships ASA's (hereafter "**MPCC"**) information- and data-driven systems are important for the company's success, and must therefore not be exposed to loss, modification or destruction.

This document describes basic security measures for the computer equipment that must be followed by all employees in MPCC. The guidelines are part of the work regulations.

1.1 Document Access

This document is distributed to all users of MPCC's IT systems.

2. USE OF DATA SERVICES

Computer systems provided by MPCC for individuals or groups for use in their work for MPCC may only be used in the performance of work related to the company, or for use in work approved by the management of MPCC. All electronic documents listed, stored, or reported by use of the company's computers are owned by MPCC or are in MPCC's custody. MPCC can access data stored on the company's computer systems when it is necessary for business or legal reasons. MPCC reserves the right to check computer systems, to ensure proper use, and to detect security breaches. MPCC's management can review the system use at any time.

2.1 Private Use of Computer Equipment

Use of MPCC computer equipment shall be work-related, but a limited private use is accepted. Private use, however, is not allowed if this for example:

- interferes with or competes with MPCC's business conduct,
- interferes with employees own or other employees work in MPCC,
- entails increased costs for MPCC,
- involves commercial request,
- provides information about or lists of MPCC's employees to unauthorized persons, and
- involves public or private distribution lists.

The use of the MPCC email system is intended for company-related/business-related activities. Occasional and sporadic private use of MPCC's email systems and access to the Internet for private use during or outside of normal working hours is, however, permitted without the approval of management, provided that none of the above-mentioned prohibitions are violated.

2.2 Chain Letters and Virus Warnings

Many forms of chain letters and virus warnings are sent and received. These can come in the form of offers of free trips or large sums of money, warnings about computer viruses or they can be related to sympathy and support actions, and you are often asked to forward this.

It is not permitted to use MPCC's computer systems to send or respond to chain letters or virus warnings. Upon receipt of a chain letter or virus warning via email, this must not be forwarded, but deleted immediately. The MPC IT department may need to be contacted for further handling.

2.3 Offensive and Inappropriate Content

MPCC's employees should not open or post content that may be considered inappropriate, offensive, or disrespectful by others. It is not possible to create a list for all such content, but some clear examples include:

- Content with sexual images or descriptions
- Content that supports illegal activities
- Content that supports intolerance towards other people

Questions regarding inappropriate or offensive content should be raised with management.

3. LEGAL CONSIDERATIONS AND SECURITY

3.1 Software Licenses

The MPC IT department is responsible for servicing and maintaining the machines and software licenses they acquire and install for employees. All installation of programs on the machines must therefore be performed by or in consultation with the MPC IT department.

It is not permitted to copy or duplicate approved software except as described in the terms and conditions of the software license.

3.2 Intellectual Property Rights, Including Copyright

Most of the information and software (programs, audio, video, data files, etc.) available to the public (including the internet) are protected by copyright or other intellectual property rights.

- The acquisition of software from such sources or use in MPCC is not permitted unless it has been approved by the copyright holder.
- All copyright restrictions on software must be read and understood. Are you in doubt that MPCC will be able to comply with the terms, the material must not be downloaded or used.

- Any expressed requirement or restriction in connection with the use of such material shall be complied with. This may, for example, be a ban on use for commercial purposes; prohibition of use or distribution where someone else is charged or subject to copyright.

3.3 Data Security

All employees shall contribute to reduce the possibility and consequences of theft of MPCC's computer resources and installations (such as desktops, laptops, PDAs, and mobile phones). Furthermore, this applies to other material such as external storage devices, CDs, written products, and information that is stored on these or in similar ways. Whether it is stored at MPCC's office, in your home office, at a client's home, in a hotel, on a plane or in a car or otherwise, the material must be properly protected.

3.3.1 Leaving the Office or Workplace Temporarily

When You Leave The Office or Workplace Temporarily

- make sure that confidential materials are not displayed on the screen, and
- protect any material that contains confidential information or take it with you.

3.3.2 Leaving the Office for the Day

When you leave the office for the day

- you shall log out of the network, and
- your computer must be switched off.

3.3.3 Traveling or Working Away from the Office or Workplace with a Notebook

- Keep your notebook in your custody if possible.
- When travelling by air, your notebook should not be checked in as luggage. Be aware of the possibility of theft when going through security checks at airports.
- When travelling by car, your notebook must be locked in the trunk of the car so that it is not visible.
- Do not leave your notebook in any empty car for a long time.
- If you must leave your notebook in a hotel, lock it in the hotel safe if available.
- If you travel with confidential MPCC equipment such as documents, external storage devices, CDs, or other storage media, this equipment must be protected in accordance with the same guidelines that apply to protecting your notebook.

Important: If your notebook or any other MPCC device is stolen or otherwise lost, this must be reported immediately to the MPC IT-department and the MPCC management.

3.4 Password

A password for access to a computer is the primary key to data-security. The password gives you unique identification and access to MPCC's computer resources. For your own security and to protect MPCC's resources, the password should be kept secret and not shared with or disclosed to others. Anyone who shares their password with others is responsible for misuse.

The following guidelines should ensure that the password is not trivial or predictable and that it will be resistant to attack by "hackers".

The password needs to be compliant with the relevant MPC IT password requirements.

When you need to change the password, you must select a new password, do not change to a previous password.

Important: If you use computer systems that are not under MPCC's control, do not select the same password on external systems that you have selected on the internal one.

3.5 Protection of Confidential Information

Confidential information shall be protected from any access or display by unauthorized persons and shall only be available to persons who have business needs to obtain the information.

3.6 Handheld Devices (iPads, Mobile Phones with Data Access, etc.)

Handheld devices are relatively small, portable devices that are used to access or store information, such as email/calendar information and internal web pages. These devices require physical and logical access control if confidential or other business sensitive data is available or stored on the device. The following measures are required:

All hand-held devices outside of MPCC's premises must always be physically under control.

3.7 Printing Confidential Information

When printing confidential information, you must protect the information from theft and unauthorized "viewers". (The term «printing» includes printers and all other devices used to make physical copies). Please note that in open areas such as switchboards, meeting rooms, and such, there may be unauthorized personnel.

3.8 Use of Phones

Please note that using telephones outside MPCC to discuss confidential information may pose a security risk. Make sure you are not overheard when discussing confidential matters.

Avoid posting confidential messages on non-MPCC voicemail systems. If you routinely use a non-MPCC voicemail system for MPCC business, you should recommend to your callers in your "welcome-message" that they do not leave confidential messages.

4. Internal Network, Internet, and Email

When you are connected to and use MPCC's internal network:

- Do not introduce yourself as any other users on the network (do not disguise yourself.
- Do not add network equipment that extends MPCC's infrastructure (for example equipment such as routers, modems, wireless access points, printers, etc.)
- Do not install software between computers without permission from the MPC IT department.

4.1 Internet

Access to internet from MPCC:

- Use only services you are authorized to use. Do not attempt to get access to Internet systems or server inputs without prior permission.

4.1.1 Inappropriate Websites

Countless websites contain or distribute material that is inappropriate in a workplace. It is impossible to list all such websites or forms of inappropriate material. However, there are some clear examples:

- Websites that contain sexual images and related material.
- Websites that encourage illegal activities.
- Websites that encourage intolerance of others.

MPCC's computer equipment shall not be used to visit such web pages or distribute or acquire similar materials from the internet. Questions regarding inappropriate web pages or offensive material can be directed to the MPC IT department. MPCC may reserve the right to carry out technical checks to prevent access to inappropriate/offensive web pages. MPCC's employees must not assume that MPCC approves all websites that are not blocked by the MPC IT technical support.

4.1.2 Privacy Online

On the internet, there is a great risk to your privacy or for leakage of information about your activities. You should be aware of the following matters regarding your privacy when surfing the web:

- When you visit a web page, the page you are visiting can identify where your internet connection originated. For example, if you use the Internet at work, your activities can be tracked to MPCC.
- Websites can log all your activities including personal data that you provide. The website owner can link you to this information to give you a better web experience, or they can gather competing information, or both. Some websites do not respect the privacy act and may make the information from you available to others.

4.2 Use of Email in MPCC

All emails sent from MPCC's official email addresses are to be regarded as the company's emails in the same way as letters sent out on the company's letterhead.

MPCC is therefore considered the sender/addressee of all emails sent from or received at MPCC official email addresses. In principle, the individual user can therefore not expect discretion for emails sent from or received to this address. Such mail is treated in the same way as ordinary letters and faxes.

4.2.1 Private Email

Although MPCC's official email addresses are meant to be used for work-related correspondence, this does not preclude sending and receiving necessary and concise messages of a private nature.

The reason for this is, firstly, technical conditions. Reference is made to section "4.2.3 Technical conditions". Secondly, when sending a private email, it will also appear that the email comes from MPCC. This indicates that you have to take into account what the email contains. MPCC does not want to be a recipient or sender of non-work-related emails containing video and/or music and/or pornography. To the extent that the individual receives such email, it must be deleted immediately.

The work environment also dictates that you do not distribute email with content that could be perceived as offensive to others.

4.2.2 Access to Other People's Emails

Everyone must ensure that their email is checked daily. If you do not have the opportunity to do so yourself due to meetings, holiday absences, illness, and such, an automatic absence notice must be used.

The company may in certain situations have the need to access employees' emails and other electronically stored material. Any such access to an employee´s email must be in accordance with the regulations in the Working Environment Act section 9 and the regulation regarding the employer's access to the email box and other electronically stored material.

4.2.3 Technical Conditions

For technical reasons, everyone must ensure that unnecessary email is not stored in the system. This especially applies to emails with attachments that pose a security risk, for example in the form of a risk of virus spread. Examples are images, videos, music files, program files, etc.

Messages with large attachments take up a lot of space in the system and increase the risk of the system being overloaded. This is especially noticeable in connection with holidays such as Christmas and easter where many send greetings with large attachments. A small video clip requires a lot of space, and even more so if this is forwarded to many employees.

The individual must at all times make sure to delete private email that contains large amounts of data so that this does not take up space in the system.

4.2.4 Logs

All authorized and unauthorized use of the information system at MPCC is registered and stored for at least three months. The same applies to all other events in the system that are important for the security of the system. The information is only used for administration of the system and to detect/solve security breaches.

4.2.5 Receiving Unsolicited Email

MPCC's employees may risk receiving (mass-sent) unsolicited email (often called spam or junk mail). Each time you use your MPCC email address, you enter information into a database that can be sold or distributed to advertising companies for mass mailing (spam). To protect yourself against this when you conduct private business on the internet, you should not register or sign up for anything using your MPCC email address. You should instead obtain a personal email address for such purposes.

4.3 Routine for Using Email in Ordinary Work

When sending an ordinary email, one does not receive a receipt when the addressee receives the email. If something goes wrong with the sending of the email, in many cases (but not in all), you will receive a return email that is generated automatically, the message that the email has not arrived.

For this reason, email cannot be used to provide notices, messages etc. that it is imperative that one can prove has arrived, typically exercises of rights/deadlines in contractual relationships.

5. REPORTING SECURITY INFRINGEMENTS

If you register a security breach, it is important that you immediately report this to MPC IT and the MPCC management.

If you have security questions, you can discuss these with the MPC IT support.