Copenhagen Malmö Port AB
Containervej 9
P.O. Box 900
DK-2100 Copenhagen

Tel +45 35 46 11 11
Fax +45 35 46 11 22
cmport@cmport.com
www.cmport.com

04. 01. 2021

Terror security of "Copenhagen Malmö Port" (version 18/ 2021)

On 1 July 2004, the International Ship and Port Facility Security Code, also known as the ISPS Code, entered into force.

The derived Danish/Swedish laws entered into force on 1 July 2004 and apply to port facilities serving the following vessels on international voyages:

Passenger ships, including high-speed craft.
Freighters.
Mobile offshore oil rigs with autonomous propulsion machinery.

The implementation of the code is to prevent port facilities from being used as a launching point for terrorists or their weapons, as well as to protect the port facility from becoming an end in itself.

CMP's security organisation is placed under the authority of the Maritime Service, physically at the Port Office, which is open 24 hours a day (tel. + 45 35 46 11 38)

CMP employees will perform the security tasks in accordance with the current

legislation. The chief security officer is Port Captain Thomas Sonne-Schmidt/

PFSO/PSO

For each facility, a vulnerability assessment has been prepared on the basis of a security plan. Depending on the vulnerability of the facility (consequence/probability) and the type of cargo handling that takes place at the facility, the security plan shall describe how the consequences are carried out:

1) access control to the facility;
2) restricted areas
3) handling of the load,
4) the supply of ship's stores,
5) handling unaccompanied baggage;
6) monitoring of the security of the port facility;

From 1 July 2004, CMP introduced the following for customers, partners and employees:

Ad 1 access control to the facility:
The primary function of the access control is to allow only those who have an errand at the facility to enter. All persons travelling to the facility must be able to identify themselves by photo ID, which may consist of a driving licence, passport or the like.

The access control may result in a interrogation and search of vehicle and cargo.

For regular users of the facility, some facilities will be subject to automatic access control systems, such as card readers and port telephone.

Visitors, repairers, etc. to ships must generally be notified to the Port Office 24 hours in advance. For brokers and companies in this field, it can be determined, in agreement with PFSO, to do so. However, CMP must have access to these documents 24 hours in advance. This also applies to crew and passenger lists.

Companies must be able to confirm a person's affiliation with the company 24 hours in advance and must be able to document an errand or affiliation with ships/companies located on the site of the facility.

Ad 2 areas with access control
Once the access control has passed, the facility's area is considered a restricted area. This means that all those in the field are subject to the rules and regulations described by the ISPS Code/Legislation. This also applies to companies that do not have ship handling.

Ad 3 handling of the load

Check in process, OCR gate
Driver arrives at the terminal and registers his arrival via app or in the self-service kiosk/boot there is located at customs. Driver registers following:

- Container delivery
- Booking number
- Seal number (manuel process)
- Empty container (manuel process)
- IMO labels

Upon arrival with an empty container, the driver must inform whether he has seen that the container is actually empty. If this is not the case, he will not be able to enter the terminal.

Then the driver drives through OCR camera portal -and pictures are taken of the container from 5 different angles, as well as of the license plate.

The system detects:

- License plate on truck
- Container number
- Possible IMO labels
- Any seals

The driver drives on to the check in gate.

If everything between entry from driver, booking in the system and what the OCR system reads in "reality" is consistent, then the boom at the check in gate, via license plate cameras, will open when the truck approaches.

If there are inconsistencies between the entry of the driver, the booking in the system or the read of the OCR system, the driver will be informed by looking at the kiosk screen that there is a discrepancy and he will be asked to leave the area again and secure the data tally.
From here it will not be possible to get the container further into the system and thus into the terminal.

This process indicates that CMP no longer checks for seal number or empty containers. The driver must meet his carrier responsibilities and ensure proper registration in the system. If there are inconsistencies between either the entered, the booking and the "reality" seen through the OCR system, the container will not be accepted into the terminal.

In case of a match between the data and the booking, a location will be displayed on screen and the driver can drive through the gate and on to the correct location on the terminal.

Ad 4 Delivery of ship stores
Ship stores shall, if possible, be notified to the Port Office at least 24 hours before delivery to the ship with the following information: Carrier, driver, vehicle registration number. These notifications can be stored at the broker, etc., provided that security staff are given access to the information 24 hours a day.

Ad 5 handling of unaccompanied baggage
Unaccompanied baggage is not handled or accepted.

Ad 6 Monitoring of port facility security
Some facilities are electronically monitored. At all locations, staff from CMP's Port Security will take random checks on people at the facility. Questions will be asked for identity and errand at the facility. Persons who cannot account for the above will be asked to leave the area if necessary with the help of the police. Anyone who has a valid business at the facility is obliged to contribute positively to this ID check.

For the above paragraphs 1 to 6, there are also 3 security levels to which the facility must be able to be lifted.

Level 1 is the level at which ships and port facilities normally operate.
Level 2 increased, this level applies as long as there is an increased security risk and
Level 3 extraordinary; this level applies during the period when there is a probability or imminent risk of a security incident.

The authorities set the levels.

As mentioned, there will be, inter alia, the following: an access control and where necessary supported by random checks in the facility areas.
In addition, the necessary monitoring equipment and measures for securing port facilities and access routes have been installed. In addition, as described, an organisation has been set up to carry out day-to-day security and administration.

For users/ customers/ employees, this will mean that the security check may cause longer in-passage time.
For employees, the new security measures mean that employees in their daily work are also aware of security within their field of work.

It is therefore important that when you are in the port area you are aware and respond as stated below and contact the CMP Port Office at tel: 3546-1138 and your own securityofficer.

What should I do?

- If you become aware of someone attempting to enter the area of operations bypassing control systems, or if you meet someone else trying to circumvent the port security measures, ask the person to leave the area and pass your observations to the Port Office at the above tel.

- If you are responsible for letting people into the ISPS area, make sure that the person is expected/ known, can account for their business and may legitimize themselves using ID cards ect. If this is not possible, do not let the person in and contact the above.

- If you detect any attempted interference with loading units, you must pass on your observations to the Port Office, as well as any own security organisation.

- If you see a person in the field who is not employed by the company and who does not have an errand in the field, or whose behaviour attracts attention (e.g. a tourist sightseeing, an angler, or a person running around), ask them to leave the port area and to report this to the Port Office, as well as any own security organisation.

- If you become aware of effects (e.g. packages, bags or things and cases) left in the port area in places where these are 'normally' not to be located, you must pass the information on to the Port Office, as well as any own security organisation.

- The pass and/or identity card provided to you gives you the right to pass control systems and to travel in certain areas of CMP. The card is for personal use only and may under no circumstances be lent or used by other persons. Also, do not let other persons in the company of you pass control systems, everybody have to use an entry card to gain access.

- You must participate in the security exercises planned and conducted in the area where you are employed at that time.

- If it is necessary to increase security in the port or within the area where you are employed at any given time, and therefore special initiatives must be taken to prevent a possible terrorist threat from being increased or implemented, you must follow the instructions given, either through your superior, the port security organisation or through public authority.

If you have any questions in connection with the above, you are welcome to contact the sub-subscriber.

Yours sincerely
Thomas Sonne-Schmidt
Port Captain PSO/PFSO Tel direct +45 3546 1130