	<p>HEALTH, SAFETY, ENVIRONMENT AND QUALITY MANAGEMENT SYSTEM</p> <p>68.0 CYBER SECURITY</p> <p>ON THE JOB TRAINING</p>	<p>OJT : 068 Page : 1 of 5 Date : 02-Sep-25 Rev : 10.1 Appr : DPA</p>
---	---	---

VESSEL : _____

DATE : _____

Training: Cyber Security

The OJT is to be read in conjunction with the company's SMS Chapter 5.3 IT Cyber Security in Office Procedure Manual.

Crew Training on Cyber security?

- Cyber security familiarization using company Form 4.1.2 upon joining
- Monthly campaigns on Cyber Security topics, Cyber Security campaigns are provided in the SHEQ/Memo/Cyber Security portal
- Ship/shore exercise on Cyber Security (uploaded in SHEQ/Memo/Cyber Security)
- Video training on Cyber Security

Where is the company procedures on cyber security addressed in SMS?


- Chapter 5.3 IT Cyber Security in HSE Procedure Manual.
- 4.1. Master Responsibility and Authority/Fleet Procedure Manual.
- Contingency Plans Manual – 42. Cyber Security, 43. OT System compromised/failed – Cyber-attack

Different types of cyber attack?

- There are two categories of cyber attacks:
 - **Untargeted attacks**, where a company or a ship's systems and data are one of many potential targets, Examples include Malware, social engineering, Phishing, water holing, scanning etc.
 - **Targeted attacks**, where a company or a ship's systems and data are the intended target. Examples include Brute Force, Spear-Phishing, Subverting the supply chain, Denial of service etc.
- The above examples are not exhaustive, the new methods keep evolving.
- Refer section 2.1 Types of Cyber attack

What are the precautions with the emails or opening an unknown link or unknown websites?

- The emails containing attachments and/or links are the most common way of attack.
- Only trusted websites have been allowed on ship's computers. Even though protection software are in place, there is cyber risk in accessing the unknown websites
- Exercise caution with the emails and attachments which may contain malicious software or links that automatically downloads malicious software e.g.

	<p>HEALTH, SAFETY, ENVIRONMENT AND QUALITY MANAGEMENT SYSTEM</p> <p>68.0 CYBER SECURITY</p> <p>ON THE JOB TRAINING</p>	<p>OJT : 068 Page : 2 of 5 Date : 02-Sep-25 Rev : 10.1 Appr : DPA</p>
---	---	---

\$1000 Walmart Gift Card

[Click Here](#)

Congratulations! A \$1000 Walmart Gift Card is waiting...

We are pleased to announce you've been selected.

Start Right Away

What are the restrictions on the use of personal devices on shipboard computers (e.g. USB, hard drives etc)?

- USB ports on ship's computers have been blocked/de-activated except bridge computer and master's laptop. Please check all computer on board to ensure that USB port are inactive and inform office if any USB port is found active.
- Personal devices USB and hard drives are not be connected on ship's computers.
- Transferring data from uncontrolled systems (Removable media) to controlled systems is not allowed as it represents a major risk of introducing malware. (Refer section 3.3.2 Procedural Protection Measures)

What are IT and OT systems?


- Information Technology (IT) system manages **the data** and covers the spectrum of technologies for information processing, including software, hardware and communication technologies. Generally refers to computers and devices (computers, tablets and mobile phones) and the systems used for office work, email and web-browsing.
- Operational Technology (OT) controls **the physical world** and is hardware and software that directly monitors/controls physical devices and processes. Generally refers to the bridge equipment e.g. ECDIS/Radars/GPS etc and engine control systems which are used to operate the ship.

How is the cyber risk caused to the OT systems?

- Historically OT systems were stand-alone systems
- As IT and OT systems are being networked with internet, it poses the cyber risk to OT systems
- The use of removable media/USB in OT system to update the data poses a cyber risk if infected removable media is used.
- Refer Appendix B - List of IT and OT systems, Cyber risk, and Control measures

What are the restrictions on accessing the ship's IT and OT systems by visitors?

- Visitors are not allowed to access the ship's IT and OT systems.
- Most of the ship's IT and OT systems are located in the restricted areas e.g. bridge, engine room as

	<p>HEALTH, SAFETY, ENVIRONMENT AND QUALITY MANAGEMENT SYSTEM</p> <p>68.0 CYBER SECURITY</p> <p>ON THE JOB TRAINING</p>	<p>OJT : 068 Page 3 of 5 Date : 02-Sep-25 Rev : 10.1 Appr : DPA</p>
---	---	---

per SSP

What is the procedure of printing the document using an external party's USB?

- External party's USB is not to be inserted into the ship's computer.
- USB is to be inserted only into the printer for printing a document. Please check printer is provided with the USB port. (Refer section 3.3.2 Procedural Protection Measures)

What is the procedure for repairing the OT systems on board?

- This is to be approved directly by the Ship Manager PRIOR to commencement of the job. The IT Manager or IT representative is to oversee the operation and remote access by the Service Provider. (Refer section 3.3.2 Procedural Protection Measures)

What is the cyber security procedure for ECDIS?

- Only dedicated USB provided by the ENC service provider is to be used for updating the ENC
- USB is to be kept in the safe custody of 2NO but rest of the deck officers must know its location
- A ship specific risk assessment on ECDIS Cyber Security conducted by bridge team and filed in NP133C
- Only company authorized technicians are allowed to check/service the ECDIS.

What are the warnings or signs and symptoms of the infected/compromised IT and OT systems?

- Unexpected pop-up, slow to respond, suspicious hard drive activity, sudden lack of storage space, missing files, crashes and error messages, high network activity, email is hijacked, browser becoming sluggish etc.
- Refer section 2.2 Signs of computer virus for details

What is remote access procedure for repairing the PC on board?"?


- Remove access to shipboard computers is allowed by IT department only.

Precautions with password?

- Password should be strong and changed periodically. Passwords should be a minimum of six (6) characters long. Use a combination of upper case & lower case characters, numbers and special symbols is recommended. (Refer section 3.3.2 Procedural Protection Measures)
- Passwords are like UNDERPANTS – Change them often, keep them private and never share them with anyone. (Refer campaign Cyber Security – Passwords)

Reporting of cyber events or cyber attacks?

- Report cyber incident (e.g. virus in computer), non-conformity, near miss just like any other event reported on board the vessel.

	<p>HEALTH, SAFETY, ENVIRONMENT AND QUALITY MANAGEMENT SYSTEM</p> <p>68.0 CYBER SECURITY</p> <p>ON THE JOB TRAINING</p>	<p>OJT : 068 Page 4 of 5 Date : 02-Sep-25 Rev : 10.1 Appr : DPA</p>
---	---	---


- Examples of such incident, non-conformities and near miss are:
 - unauthorised access to ship's IT and OT Systems, unauthorized use of administrator privileges, suspicious network activity, unauthorised use of removable media, unauthorised connection of personal devices to ship's computer, disruption to the IT/OT systems
- Refer section 3.3.3 Detecting and reporting of cyber event
- Every crew member is responsible for alerting the Master of any possible or potential cyber risks noted while they using the company IT infrastructure.
- Incident is to be reported to office using 24 hrs contact number and IT department, refer company communication card provided in emergency contingency plan manual.

Procedure in case of IT and/or OT system is compromised/failed or action to be taken after cyber attack?

- Activate contingency plan pertaining to the compromised equipment
- Refer contingency Plans Manual – 42. Cyber Security, 43. OT System compromised/failed – Cyber attack

Following are few examples of the of poor cyber hygiene which may attract PSC deficiency:

- Poor cyber hygiene
- Username / Password openly displayed
- Computer system appears to require a generic login or no login for access
- Computer system does not appear to automatically log out after extended period of user inactivity
- Heavy reliance on flash drive/USB media use
- Unauthorized access to the computers is being allowed
- External drive/USB connected to the shipboard computers
- Dedicated USB is not being used to update the ECDIS
- The dedicated USB for ECDIS is lying on the table
- Lack of awareness with the cyber security protection measures for ECDIS

	<p>HEALTH, SAFETY, ENVIRONMENT AND QUALITY MANAGEMENT SYSTEM</p> <p>68.0 CYBER SECURITY</p> <p>ON THE JOB TRAINING</p>	<p>OJT : 068 Page 5 of 5 Date : 02-Sep-25 Rev : 10.1 Appr : DPA</p>
---	---	---

Above read and understood:

CNO: _____

2NO: _____

3NO: _____

X2NO/X3NO _____

Deck Cadet _____

2EO _____

3EO _____

4EO _____

EEO _____

Engine Cadet _____

Ratings : Attach signed crew list

Verified by: Master / _____

Date: _____

Feedback: