Grant Agreement Number: *833389*

Project acronym: Cyber-MAR

Project full title: Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain

Syllabus

Online Training "Managing Cybersecurity"

ENTRY LEVEL

COURSE: Managing Cybersecurity

DELIVERY DATE: 16th June 2021 - 13:00 – 16:00 (CET)

COURSE DESCRIPTION: The training course is designed to develop understanding and awareness of Cybersecurity risk management and related to the Cyber-MAR concept.

This course is intended to equip an understanding of how cybersecurity risks affect management decision-making, providing insights into the risk management framework and critical aspects of cybersecurity, helpful in addressing vulnerabilities in the maritime sector.

The training is for managers who need to increase their knowledge to make informed decisions on risk assessment and management.

The objectives are to increase basic knowledge and awareness of maritime risk management processes allowing the participants to understand cybersecurity threats and manage risk.

DELIVERY MODALITY: E-LEARNING CLASS

DURATION: 3 hours

PREREQUISITE: Knowledge about Maritime and Port procedures, IT

Management, Security Management

CONTENTS

1. Cyber security fundamentals and Maritime cyber security peculiarities
2. Principles of cyber risk management
3. Threats and vulnerabilities
4. Hardware, software, humans

5. Systems and data inventory, risk assessment scope, responsibilities

6. Basics of Responding to and recovering from cyber attacks

7. Identify, Protect, Detect, Respond and Recover

✓ Final Training evaluation

TRAINING STRUCTURE
The training will be delivered online through zoom.
The attendees will receive via email an invitation zoom link to join the training.

LEARNING OUTCOMES
The participants will develop knowledge and skills necessary to understand the principles of:

▪ Remaining aware of evolving technical infrastructures Using critical thinking to analyse organizational patterns and relationships

▪ Risk management processes

▪ Cybersecurity and privacy principles

▪ Cyber threats and vulnerabilities

▪ Specific operational impacts of cybersecurity lapses

▪ Cybersecurity and privacy used to manage risks related to the use, processing, storage, and transmission of information or data

▪ Incident response and handling methodologies risks

▪ Industry-standard and organizationally accepted

▪ Resource management principles and techniques

▪ Information security program management and project management principles and techniques

▪ Enterprise incident response program, roles, and responsibilities

- Critical infrastructure systems with information communication technology that were designed without system security considerations