€ TRAINING

Marine Security Management and Control as per ISPS Code

Marine Security Management and Control as per ISPS Code

Introduction:

The Marine Security Management and Control program, under the ISPS Code, enhances security measures in maritime settings through structured protocols. It equips participants with skills to ensure compliance and protect maritime assets from threats.

Program Objectives:

At the end of this program the participants will be able to:

- Define the nature of their facility and how they are affected by the requirements of the ISPS code.

- Identify the mandatory and guidance regulations of the ISPS code.

- Develop risk assessment tools towards the Port Facility Security Assessment PFSA.

- Construct the 3 levels of the Port Facility Security Plan PFSP with enhanced knowledge of security issues.

- Operate and interact with the port facility security plan with the ships security officer and ships master.

Targeted Audience:

- Security personnel in maritime environments.

- Port facility managers and operators.

- Individuals responsible for implementing security protocols.

- Personnel involved in ship operations and management.

Program Outlines:

Unit 1:

The Background to the International Maritime Security Framework:

- Who the code applies to: Identifying the entities subject to ISPS Code regulations.

- Types of port facilities: Categorizing the various kinds of port infrastructure.

- Protection categories: Classifying security levels and measures.

- Understanding the ISPS code: Grasping the framework and objectives of the ISPS Code.

- Relevant international conventions, codes, and recommendations: Exploring associated regulations and guidelines.

- Parts of the ISPS code: Comprehending the structure and components of the ISPS Code.

Unit 2:

Recognition and Detection of Weapons, Dangerous Substances and Devices:

- Firearms.

- Low and High explosives.

- Incendiary devices.

- Grenades.

- Detonators.

- Timers and Batteries.

- Timer power units.

Unit 3:

Introduction to Port Facility Security:

- Security Administration: Overseeing the implementation and management of security protocols.

- Responsibilities and Functions of Security Organizations: Defining the roles and duties of security entities.

- Handling Sensitive Security-Related Information: Safeguarding confidential data to prevent breaches.

- Knowledge of Current Security Threats and Patterns: Staying updated on evolving risks and attack strategies.

- Techniques Used to Circumvent Security: Identifying methods adversaries use to bypass defenses.

- Security Equipment and Systems: Utilizing technology for protection, surveillance, and access control.

- Characteristics and Behavioral Patterns of Persons Likely to Threaten Security: Recognizing signs of potential threats through behavioral analysis and profiling.

Unit 4:

Port Facility Security Assessment:

- Risk assessment 4: 2: 1

- Risk assessment methodology.

- Key point identification CARVER.

- Evacuation planning.

- Search planning.

Unit 5:

Port Facility Security Plan

- Case study development of security Level 1.

- Case study development of security Level 2.

- Case study development of security Level 3.