



Training Course



Marine Security Management and Control as per ISPS Code

Description

The Maritime Security Management & Control as per ISPS Code course at Global Horizon provides a comprehensive understanding of the International Ship and Port Facility Security (ISPS) Code. The ISPS Code was developed in response to increasing security threats, particularly after the 9/11 attacks, and is implemented through Chapter XI-2 of the SOLAS Convention. This course aims to equip participants with the knowledge and skills to assess risks, implement security measures, and ensure compliance with ISPS regulations.

Objectives

- Understand the scope and impact of the ISPS Code on port facilities.
- Identify mandatory regulations and recommended guidelines within the ISPS Code.
- Develop risk assessment tools for Port Facility Security Assessment (PFSA).
- Construct and implement the three levels of the Port Facility Security Plan (PFSP).
- Effectively interact with Ship Security Officers (SSOs) and ship masters.

Who Should Attend?

- Port Facility Security Officers (PFSOs)
- Maritime Security Personnel
- Port Managers and Administrators
- Shipping Company Security Officers (CSOs)
- Government and Regulatory Officials
- Anyone involved in maritime security at port facilities

Course Outline

Day 1: Introduction to Maritime Security & ISPS Code

- Overview of international maritime security frameworks
- Application and scope of the ISPS Code
- Roles and responsibilities of contracting governments and recognized security organizations (RSOs)
- Responsibilities of Port Facility Security Officers (PFSOs)

Day 2: Recognition and Detection of Threats

Identifying weapons, explosives, and hazardous substances



- Understanding different types of security threats
- Case studies on past security breaches and incidents

Day 3: Port Facility Security Management

- Security administration and organizational responsibilities
- Handling sensitive security-related information
- · Recognizing current security threats and circumvention techniques
- Security equipment and communication systems

Day 4: Port Facility Security Assessment (PFSA)

- Risk assessment methodologies and key point identification (CARVER technique)
- Evacuation and emergency response planning
- Security search planning and execution

Day 5: Developing and Implementing Port Facility Security Plans (PFSP)

• Case study: Security Level 1 implementation

• Case study: Security Level 2 implementation

Case study: Security Level 3 implementation