Port and Maritime Terminal Security (ISPS Code) Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Port and maritime terminal security has become increasingly critical as global trade expands and complex supply chains rely on secure, resilient, and compliant infrastructure. The growing threats of terrorism, piracy, smuggling, cyber-attacks, and unauthorized access demand strong security frameworks rooted in the International Ship and Port Facility Security (ISPS) Code. Port and Maritime Terminal Security (ISPS Code) Training Course equips participants with strong security strategies, risk assessment techniques, regulatory compliance requirements, and operational protocols required to safeguard maritime terminals and port environments. Through trending industry concepts, advanced security procedures, and real-world incident analysis, participants gain the technical and managerial expertise required to strengthen port security operations.

The course provides comprehensive insights into port facility assessments, maritime threat management, emergency response planning, perimeter control, cargo screening, surveillance systems, and cybersecurity integration within maritime infrastructure. Participants develop critical competencies in coordinating port security plans, enhancing situational awareness, overseeing security personnel, and collaborating with maritime stakeholders. By the end of the training, learners will be equipped to implement effective port security measures aligned with international standards, ensuring safe, efficient, and compliant maritime operations.

Programme Curriculum

Port and Maritime Terminal Security (ISPS Code) Training Course

Introduction

Port and maritime terminal security has become increasingly critical as global trade expands and complex supply chains rely on secure, resilient, and compliant infrastructure. The growing threats of terrorism, piracy,

smuggling, cyber-attacks, and unauthorized access demand strong security frameworks rooted in the International Ship and Port Facility Security (ISPS) Code. Port and Maritime Terminal Security (ISPS Code) Training Course equips participants with strong security strategies, risk assessment techniques, regulatory compliance requirements, and operational protocols required to safeguard maritime terminals and port environments. Through trending industry concepts, advanced security procedures, and real-world incident analysis, participants gain the technical and managerial expertise required to strengthen port security operations.

The course provides comprehensive insights into port facility assessments, maritime threat management, emergency response planning, perimeter control, cargo screening, surveillance systems, and cybersecurity integration within maritime infrastructure. Participants develop critical competencies in coordinating port security plans, enhancing situational awareness, overseeing security personnel, and collaborating with maritime stakeholders. By the end of the training, learners will be equipped to implement effective port security measures aligned with international standards, ensuring safe, efficient, and compliant maritime operations.

Course Objectives

1. Understand fundamental principles and regulatory requirements of the ISPS Code.
2. Conduct comprehensive port and terminal security risk assessments.
3. Strengthen maritime threat detection through modern surveillance and intelligence tools.
4. Implement advanced access control systems for secure port environments.
5. Coordinate port facility security plans (PFSPs) aligned with global best practices.
6. Apply trending incident management and emergency response techniques.
7. Enhance cargo screening and inspection procedures for high-risk shipments.
8. Integrate cybersecurity protocols with physical port security operations.
9. Strengthen collaboration between port authorities, security agencies, and stakeholders.
10. Monitor and audit port security performance using key compliance metrics.
11. Develop strong training programs for port security personnel.
12. Implement crisis communication and information-sharing strategies during threats.
13. Promote a culture of proactive security and continuous improvement.

Organizational Benefits

- Enhanced compliance with ISPS Code and global maritime security standards
- Reduced security incidents through proactive threat management
- Strengthened coordination between port stakeholders and security agencies
- Improved cargo safety and reduced risks of illegal trafficking
- Increased operational efficiency through streamlined security procedures
- Enhanced reputation as a secure and compliant maritime gateway
- Stronger cybersecurity integration in port operations
- Reduced insurance and operational risk costs
- Increased resilience against emergencies and disruptions
- Improved confidence from global shipping partners and regulators

Target Audiences

- Port facility security officers and maritime security personnel
- Terminal managers and port operations supervisors
- Maritime regulatory authorities and government agencies
- Coast guard and navy security professionals

- Customs and border protection officers
- Shipping line compliance and security teams
- Risk management, crisis response, and emergency teams
- Logistics, cargo handling, and supply chain security professionals

Course Duration: 10 days

Course Modules

Module 1: Introduction to ISPS Code and Maritime Security

- Overview of global maritime security frameworks
- Understanding ISPS Code structure and requirements
- Roles and responsibilities of port facility security officers
- Security levels and their operational implications
- Key ISPS Code documentation requirements
- Case Study: Compliance gaps identified during a port security audit

Module 2: Port Facility Security Assessments

- Conducting threat and vulnerability assessments
- Identifying critical assets in port environments
- Evaluating physical, operational, and human-factor risks
- Applying quantitative and qualitative assessment tools
- Integrating assessment findings into security plans
- Case Study: Port vulnerability mapping after security incident

Module 3: Port Facility Security Plans (PFSPs)

- Core components of an effective PFSP
- Writing, reviewing, and updating PFSPs
- Aligning PFSPs with ISPS Code requirements
- Coordinating PFSP implementation across units
- Ensuring documentation accuracy for compliance audits
- Case Study: PFSP redesign in response to new threats

Module 4: Access Control and Perimeter Security

- Access management for vehicles, personnel, and cargo
- Perimeter fencing, intrusion detection, and barriers
- Credential verification and ID management
- Visitor management procedures
- Security screening at entry points
- Case Study: Unauthorized access leading to operational disruption

Module 5: Surveillance and Monitoring Technologies

- CCTV installation and monitoring techniques
- Integration of radar, sensors, and thermal imaging
- Real-time monitoring and security control rooms
- Automated security alerts and response workflows
- Maintenance and testing of surveillance systems

- Case Study: Surveillance gaps exploited during a breach

Module 6: Cargo Security and Screening Procedures

- High-risk cargo identification
- Non-intrusive inspection technology
- Container sealing and tracking systems
- Screening protocols for dangerous goods
- Customs–security collaboration
- Case Study: Detection of contraband through advanced screening

Module 7: Maritime Threat Awareness and Intelligence

- Identifying emerging maritime security threats
- Intelligence gathering and information-sharing practices
- Risk indicators for terrorism, smuggling, and piracy
- Behavioral detection techniques
- Collaboration with national and international agencies
- Case Study: Threat intercepted through shared intelligence

Module 8: Security Personnel Roles and Competencies

- Core duties of security teams in port terminals
- Training requirements and certification standards
- Supervisory responsibilities of PFSOs
- Behavioral and scenario-based decision-making
- Performance monitoring and evaluation
- Case Study: Security personnel response failure analysis

Module 9: Communications and Reporting

- Security communication protocols and equipment
- Incident reporting standards and best practices
- Inter-agency communication frameworks
- Radio, digital, and encrypted communication systems
- Documentation for compliance inspections
- Case Study: Communication breakdown during an emergency

Module 10: Emergency Response and Incident Management

- Developing port emergency response plans
- Evacuation, containment, and recovery procedures
- Coordination with emergency services
- Crisis command structure in port settings
- Simulated emergency exercises
- Case Study: Response to a fire outbreak in a marine terminal

Module 11: Cybersecurity in Maritime Environments

- Cyber risks affecting port and terminal systems
- Protection of operational technologies (OT) and IT systems
- Cyber incident identification and recovery

- Secure integration of digital logistics systems
- Cybersecurity awareness for port personnel
- Case Study: Cyber-attack disrupting port operations

Module 12: Security for Waterfront and Vessel Interface

- Vessel–port interface risk zones
- Waterside patrols and surveillance
- Vessel identification and clearance procedures
- Securing berths and waterfront facilities
- Coordination with ship masters and port control
- Case Study: Breach through unsecured waterfront access

Module 13: Screening of People and Crew Security

- Passenger and crew screening methods
- Identity verification and biometric systems
- Screening equipment and detection technologies
- Managing high-traffic terminal flows
- Collaboration with immigration authorities
- Case Study: Crew member security violation incident

Module 14: Compliance Monitoring and Security Audits

- Conducting internal and external ISPS Code audits
- Performance measurement and metrics
- Corrective actions and continuous improvement
- Audit documentation and reporting
- Inspector expectations and compliance checklists
- Case Study: Port failing an external ISPS inspection

Module 15: Building a Security Culture in Port Operations

- Promoting awareness among port staff
- Implementing continuous training and drills
- Encouraging incident reporting and accountability
- Leadership commitment to security values
- Integrating security into daily port operations
- Case Study: Culture change leading to reduced incidents

Training Methodology

- Interactive instructor-led presentations
- Group discussions and problem-solving exercises
- ISPS Code document review and interpretation
- Real-world case study analysis
- Practical simulations and scenario-based activities
- Development of action plans for port security improvement

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com