Port Facility Security Plan 2019 - 2024

Comprising the Port Facility Security Plan pursuant to Regulation (EC) No 725/2004 (ISPS) – to be completed by Art. 2.4 Port Facilities and Port Facilities in “Multi Facility” Ports

Port Name:

Port Facility Name & Address:

Date:

Issue Number:

Approval Date:

Date of last review:

Restricted when Completed
Table of Contents

Overview & Background ......................................................................................................................... 4
Glossary & Definitions ............................................................................................................................... 5
Distribution & Amendment Records .......................................................................................................... 6
Executive Summary ................................................................................................................................. 7
Chapter 1 Port Facility General Information .......................................................................................... 8
  1.1 Port Facility General Information .................................................................................................... 9
  1.2 Port Facility Structural and operational information ....................................................................... 10
  1.3 Organisational Structure ................................................................................................................ 11
Chapter 2 Management of Security Procedures ..................................................................................... 12
  2.1 Security Level Changes .................................................................................................................... 13
  2.2 Duties of Port Facility Security Personnel and other port facility personnel on security aspects ...... 14
  2.3 Port Facility Security Plan Review, Amendment & Audit ................................................................. 15
  2.4 Government Officials requiring access ......................................................................................... 16
  2.5 Reporting of and response to Security Threats, Incidents & Breeches ............................................ 17
  2.6 Document & information security ................................................................................................. 18
  2.7 Operation, Testing, Calibration and Maintenance of Security Equipment .................................... 19
  2.8 Security Training ............................................................................................................................ 20
  2.9 Security Drills & Exercises ............................................................................................................ 21
  2.10 Evacuation Procedures ................................................................................................................. 22
Chapter 3 Communication ........................................................................................................................ 23
  3.1 Ship & Port Facility Communication Links .................................................................................... 24
  3.2 Ship Security Alert .......................................................................................................................... 25
  3.3 Ship Security Incident ..................................................................................................................... 26
  3.4 Port Facility Security Incident ....................................................................................................... 27
  3.5 Information to be provided by Ships ............................................................................................... 28
  3.6 Reporting procedures to Government ............................................................................................ 29
  3.7 Vetting & Screening of personnel with a “Need to Know” ............................................................. 30
Chapter 4 Measures at Security Level 1 ................................................................................................. 31
  4.1 Physical Security ............................................................................................................................. 32
  4.2 Access to the Port Facility ................................................................................................................ 33
  4.3 Check & Search procedures ............................................................................................................. 34
  4.4 Designated Restricted Areas ........................................................................................................... 35
  4.5 Designated Controlled Buildings ................................................................................................... 36
  4.6 Security of Cargo and the cargo handling equipment ................................................................. 37

Restricted when Completed

port facility security plan template 2019 -2024
Chapter 7 Port Facility Security Standard Operating Procedures (Additional SOP’s may be utilised as designated in the PFSP)

SOP 1. Action for Receipt of Phone Bomb Threat .......................................................... 59
SOP 2. Search and Verification Procedure .................................................................... 60
SOP 3. Actions if a Suspicious Object / Device is found .............................................. 61
SOP 4. Actions if a Ship is Hijacked within a Port Facility ........................................... 62
SOP 5. Actions on Discovering a Suspicious Postal / Courier Item ......................... 63
SOP 6. Initiation of Relevant Emergency / Major Incident Plan ................................. 64
SOP 7. Action for Discovery of Suspicious Persons ..................................................... 65


Annex A - Photos, Maps & Charts .............................................................................. 67
Annex B – Bomb Threat Checklist ................................................................................ 68
Annex C – Listing of Tenants & adjacent users .............................................................. 69
Overview & Background


To complement the above changes, enhancements to the “SafeSeasIreland” system have been made, so as to enable the submission of relevant documentation by secure electronic means.

This template has been amended to take account of horizontal issues identified during inspections at port facilities by the E.C and the Administration and to take account of emerging threats from cyber, UAV’s etc.

Further reviews of these arrangements will be undertaken so as to take account of experience gained and to ensure all regulatory requirements continue to be fulfilled.

The security plans and assessments may be examined by the European Commission and all ports and port facilities may be subject to inspection and audit by the EC during the period of validity.

This PFSP template should be used for:

- “Article 2.4 Single Facility” Ports where an approved assessment confirms that the boundaries of the Port and the Facility are the same. These facilities will continue to be subject to the requirements of the Regulation only (as per Art 2.4 of Directive 2005/65/EC) and will only require a Port Facility Security Plan, to be submitted for approval via SSI as per previous arrangements.
- Individual Port Facilities in multi-facility ports.*

In single facility ports where Art. 2.4 does not apply, a “Combined” Port Security Plan may alternatively be adopted, which includes the requirements of both the EU Regulation and the EU Directive.

*The Port Security Officer will be responsible for the creation of an overall port security plan for a port, comprising all facilities and port areas for the attention of the Port Security Authority. This will subsequently be uploaded to the SafeSeasIreland system for approval by the Administration.

Brian Hogan
Chief Surveyor
Irish Maritime Administration
**Glossary & Definitions**

**Port:** any specified area of land and water with boundaries defined by the Member State in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport operations.

**Port Boundary:** the security boundary around a port to include not just the entire operational and legal boundary of the port, but also any adjacent buildings, infrastructure or operations which might have a negative impact on port operation, should a security incident occur involving such buildings, operations or infrastructure.

**Ship/Port interface:** interactions that occur when a ship is directly and immediately affected by actions involving the movement of persons or goods or the provision of port services to or from a ship.

**Port Facility:** location where the ship/port interface takes place. This includes areas such as anchorages, waiting berths and approaches from seaward.

**Port Security Authority:** Member States shall designate a Port Security Authority for each port. A Port Security Authority may be designated for more than one port.

**Port Security Officer (PSO):** A Port Security Officer shall be approved by the Member State as per Directive 2005/65 EC. Each port, where practical, shall have a different Port Security Officer, but may, if appropriate, share a Port Security Officer.

**Port Facility Security Officer (PFSO):** the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers as per Regulation 725/2004.

**Port Facility Security Assessment:** Each port facility security assessment shall be carried out taking into account as a minimum the detailed requirements laid down in Regulation 725/2004. Port facility security assessments may be carried out by a recognised security organisation. Port facility security assessments shall be approved by the member state concerned. PFSA’s are to be completed using a template approved by the Administration.

**Port Security Assessment:** Each port security assessment shall be carried out taking into account as a minimum the detailed requirements laid down in Annex I of Directive 2005/65/EC. Port security assessments may be carried out by a recognised security organisation. Port security assessments shall be approved by the member state concerned. Port security assessments are to be completed using a template approved by the Administration.

**Security Level 1:** the level for minimum appropriate protective security measures shall be maintained at all times.

**Security Level 2:** the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of a heightened risk of a security incident.

**Security Level 3:** the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.
Distribution & Amendment Records

Distribution Record

<table>
<thead>
<tr>
<th>Date</th>
<th>Copy No</th>
<th>Issued to</th>
<th>Hard / Soft copy</th>
<th>Location held</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Amendment Record

<table>
<thead>
<tr>
<th>Date Amended</th>
<th>Amendment</th>
<th>Chapter &amp; Page ref</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 1 Port Facility General Information

1.1 General Information

1.2 Port Facility Structural and operational information

1.3 Organisational Structure
### 1.1 Port Facility General Information

<table>
<thead>
<tr>
<th></th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name of Port Facility</strong> (&amp; any alternative name)</td>
<td></td>
</tr>
<tr>
<td><strong>PSO name &amp; contact details</strong></td>
<td></td>
</tr>
<tr>
<td><strong>PFSO name &amp; contact details</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Is there an alternative PFSO</strong></td>
<td>Yes ☐ No ☐</td>
</tr>
<tr>
<td><strong>If Yes, give details</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name &amp; contact of Recognised Security Organisation</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Name and contact details of local Garda Station / Crime prevention officer</strong></td>
<td></td>
</tr>
<tr>
<td><strong>24HR Emergency Contact Numbers</strong></td>
<td></td>
</tr>
</tbody>
</table>
### 1.2 Port Facility Structural and operational information

<table>
<thead>
<tr>
<th>Size and brief description of port facility including sub areas</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Berths and vessel types</td>
<td></td>
</tr>
<tr>
<td>Origins &amp; destinations of cargo shipped through port facility</td>
<td></td>
</tr>
<tr>
<td>Does the port facility handle Dangerous Goods? If yes, give details</td>
<td>Yes [ ] No [ ]</td>
</tr>
</tbody>
</table>
1.3 Organisational Structure

Identify all organisational aspects relevant to overall port security
Chapter 2 Management of Security Procedures

2.1 Security Level Changes

2.2 Duties of Port Facility Security Personnel and other port facility personnel on security aspects

2.3 Port Security Plan Review, Amendment & Audit

2.4 Government Officials requiring access

2.5 Reporting of and response to Security Threats, incidents & breeches

2.6 Document & information security

2.7 Operation, Testing, Calibration and Maintenance of Security Equipment

2.8 Security Training

2.9 Security Drills & Exercises

2.10 Evacuation Procedures
2.1 Security Level Changes

List the procedures to follow in the event of a change in security level, both during normal working hours and out of hours.

Tables / bullet format only
2.2 Duties of Port Facility Security Personnel and other port facility personnel on security aspects

Explain the role of security personnel and their reporting procedures and for other personnel regarding security aspects. (Refer to ISPS Code Part A, Section 17.2)

Tables / bullet format only
2.3 Port Facility Security Plan Review, Amendment & Audit

List of procedures

Tables / bullet format only
2.4 Government Officials requiring access

Procedures for dealing with Government Officials

Tables / bullet format only
2.5  **Reporting of and response to Security Threats, Incidents & Breaches**

List of procedures for response to threats (including cyber threats and UAV’s etc.), Incidents and Breaches and reporting of same

Tables / bullet format only
2.6 **Document & information security**
Outline how information and documents are secured

Tables / bullet format only
2.7 Operation, Testing, Calibration and Maintenance of Security Equipment

Outline the operation, testing, calibration and maintenance of security equipment – Calibration and maintenance to be carried out by a licenced contractor

Tables / bullet format only
2.8 **Security Training**

Provide training requirements for all staff, list of courses only – please keep training records separate

Tables / bullet format only
2.9 Security Drills & Exercises

Drills are defined as practising the participants in their roles and responsibilities.

Exercises are defined as testing the processes and procedures as well as practising the participants in their roles and responsibilities. They will consist of a series of actions within a broad scenario designed to test procedures and participants in a varying degree of urgency or dilemma. Exercises, where possible, should include the Port Tenants, adjacent infrastructure, ships alongside, Local Authorities & Law Enforcement Agencies.

The Port Facility Operator shall forward to the Marine Survey Office no later than the 31st January each year, a provisional yearly schedule of Drills & Exercises it intends to conduct.

Individual drill & exercise reports shall be kept separate from the Plan.

Tables / bullet format only
2.10  Evacuation Procedures
Remote assembly points to be specified in addition to normal assembly point.

Outline security procedures and maintenance in the event of evacuation from the Port Facility & Ships

Details of muster points

Tables / bullet format only
Chapter 3 Communication

3.1 Ship & Port Facility Communication Links

3.2 Ship Security Alert

3.3 Ship Security Incident

3.4 Port Facility Security Incident

3.5 Information to be provided by Ships

3.6 Reporting procedures to Government

3.7 Vetting & Screening of personnel with a “Need to Know”
3.1 **Ship & Port Facility Communication Links**

Provide details of communication links with ships including backup

Details of communication links between port facility personnel with security duties

Tables / bullet format only
3.2  **Ship Security Alert**
Details of procedures following a ship security alert alongside and at sea

Procedures for handling false alarms

Tables / bullet format only
3.3 **Ship Security Incident**

Action taken in the event of a ship security incident (Personnel & authorities to be informed)

- Procedures for handling false alarms
- Protection of communications hub

Tables / bullet format only
3.4 Port Facility Security Incident

Action taken in the event of a Port facility security incident (Personnel & authorities to be informed)

Procedures for handling false alarms

Protection of communications hub

Tables / bullet format only
3.5 **Information to be provided by Ships**

Procedure for pre-arrival information. (To include measures to ensure that ISPS vessels without a pre-arrival report in SSI are not permitted to berth at the port facility)

Procedure for a Declaration of Security

Action to be taken when the ship is at a higher level security than the port facility

Procedures for dealing with SOLAS ships without a valid security certificate

Tables / bullet format only
3.6 Reporting procedures to Government
Changes to security level reports and procedures for informing relevant officials

Tables / bullet format only
3.7 Vetting & Screening of personnel with a “Need to Know”
Details of procedures followed in obtaining background and current relevant information about personnel entrusted with security sensitive information

It is recommended that the screening process adheres to the British Standard 7858:2012

All security service providers will be required to comply with The Private Security Services Act 2004
Chapter 4 Measures at Security Level 1

4.1 Physical Security

4.2 Access to the Port Facility

4.3 Check & Search procedures

4.4 Designated Restricted Areas (including monitoring to ensure only authorised persons have access)

4.5 Designated Controlled Buildings

4.6 Security of Cargo and the cargo handling equipment

4.7 Monitoring of security of the port facility
4.1 **Physical Security**
List physical security measures at normal security level

Include all fences, lighting, cameras etc.
4.2 **Access to the Port Facility**

Include all access gates, Entry control points, ID clearance, types of passes etc.
4.3 **Check & Search procedures**

Include procedures for ship’s crew & shore leave

Checking procedures for persons

Checking procedures for baggage & unaccompanied luggage

Checking procedures for vehicles, cargo & freight

Checking procedures for ships stores

Procedures for recording information
### 4.4 Designated Restricted Areas

List of restricted areas (permanent & temporary)
4.5 Designated Controlled Buildings

Any areas designated as a controlled building
4.6 Security of Cargo and the cargo handling equipment

Procedures for the security of cargo & cargo equipment
4.7 Monitoring of security of the port facility

Procedures for monitoring security & list of resources used.

Include all physical security monitoring equipment
Chapter 5 Measures at Security Level 2

5.1 Physical Security
5.2 Access to the Port Facility
5.3 Liaison with Port Tenants and Owners/operators of adjacent infrastructure
5.4 Check & Search procedures
5.5 Designated Restricted Areas
5.6 Designated Controlled Buildings
5.7 Security of Cargo and the Cargo handling equipment
5.8 Monitoring of security of the port facility
5.1 Physical Security

Include only information for additional security measures, over and above those mentioned at Security Level 1.
5.2 **Access to the Port Facility**

Include only information for **additional security measures**, over and above those mentioned at Security Level 1.
5.3 Liaison with Port Tenants and Owners/operators of adjacent infrastructure

Outline any agreed procedure for contacting tenants and adjacent users in the event of increased security
5.4 Check & Search procedures
Include only information for additional security measures, over and above those mentioned at Security Level 1
5.5 **Designated Restricted Areas**

Any additional areas that will be restricted in the event of an increase in security

Extra security measures for at restricted areas
5.6 Designated Controlled Buildings
Include only information for additional security measures, over and above those mentioned at Security Level 1.
5.7 **Security of Cargo and the Cargo handling equipment**

Include only information for *additional security measures*, over and above those mentioned at Security Level 1.
5.8 Monitoring of security of the port facility

Include only information for additional security measures, over and above those mentioned at Security Level 1.
Chapter 6 Measures at Security Level 3

6.1 Physical Security

6.2 Access to the Port Facility

6.3 Liaison with Port Tenants and Owners/operators of adjacent infrastructure

6.4 Check & Search procedures

6.5 Designated Restricted Areas

6.6 Designated Controlled Buildings

6.7 Security of Cargo and the Cargo handling equipment

6.8 Monitoring of security of the port facility

6.9 Emergency Closure
6.1 **Physical Security**

Include only information for additional security measures, over and above those mentioned at Security Level 2.
6.2 **Access to the Port Facility**

Include only information for *additional security measures*, over and above those mentioned at Security Level 2.
6.3  Liaison with Port Tenants and Owners/operators of adjacent infrastructure

Include only information for additional security measures, over and above those mentioned at Security Level 2.
6.4 Check & Search procedures
Include only information for additional security measures, over and above those mentioned at Security Level 2
6.5 Designated Restricted Areas
Include only information for additional security measures, over and above those mentioned at Security Level 2.
6.6 Designated Controlled Buildings

Include only information for additional security measures, over and above those mentioned at Security Level 2.
6.7 **Security of Cargo and the Cargo handling equipment**

Include only information for [additional security measures](#), over and above those mentioned at Security Level 2.
6.8 Monitoring of security of the port facility

Include only information for additional security measures, over and above those mentioned at Security Level 2.
6.9 **Emergency Closure**

Procedures for ceasing port operations upon request by Government Officials/Authorities

Procedures for denying access to the port or port facilities
Chapter 7 Port Facility Security Standard Operating Procedures (Additional SOP’s may be utilised as designated in the PFSP)

SOP 1. Action for Receipt of Phone Bomb Threat

SOP 2. Search and Verification Procedure

SOP 3. Actions if a Suspicious Object / Device is found

SOP 4. Actions if a Ship is Hijacked within a Port Facility

SOP 5. Actions on Discovering a Suspicious Postal / Courier Item

SOP 6. Initiation of Relevant Emergency / Major Incident Plan

SOP 7. Action for Discovery of Suspicious Persons

SOP 8. Cyber Risk Management Procedures
SOP 1. Action for Receipt of Phone Bomb Threat
SOP 2. Search and Verification Procedure
SOP 3. Actions if a Suspicious Object / Device is found
SOP 4. Actions if a Ship is Hijacked within a Port Facility
SOP 5. Actions on Discovering a Suspicious Postal / Courier Item
SOP 6. Initiation of Relevant Emergency / Major Incident Plan
SOP 7. Action for Discovery of Suspicious Persons
SOP 8. Cyber Risk Management Procedures
Annex A - Photos, Maps & Charts

Provide up to date aerial photographs, maps, drawings, plans & charts outlining the delineation of the port facility boundary (the Ship/Shore interface boundary as per EU Regulation 725/2004,) the facility’s legal boundary if different and Admiralty Charts showing adjacent water approaches to the facility

Include descriptions of Restricted Areas and Controlled Buildings
Annex B – Bomb Threat Checklist
<table>
<thead>
<tr>
<th>Tenant Name &amp; Nature of Business</th>
<th>Tenant Contact Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Adjacent Users Name &amp; Nature of Business</td>
<td>Adjacent User Contact Number</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>