Republic of Latvia

Cabinet

Regulation No. 746

Adopted 22 December 2015

**Regulations Regarding the Division of Functions, Implementation and Supervision of Ships, Companies, Ports and Port Facilities Security**

*Issued pursuant to*

*Section 17, Paragraph four and Section 19, Paragraph five of the Maritime Administration and Marine Safety Law*

**1. General Provisions**

1. This Regulation prescribes:

1.1. division of functions, procedures for implementation and supervision of ships and companies, ports and port facilities security laid down in international laws and regulations;

1.2. rights and obligations of the State joint stock company “Maritime Administration of Latvia” (hereinafter – the Maritime Administration), the Ship and Port Security Inspectorate (hereinafter – the SPSI) and the Maritime Safety Inspectorate (hereinafter – the MSI);

1.3. requirements for obtaining the International Ship Security Certificate, Interim International Ship Security Certificate, Statement of Security Compliance of the Ports and Port Facilities, and also procedures for issuing and revocation of these certificates and their statements;

1.4. requirements for approval of training programmes for port or port facility personnel and the procedures for their approval;

1.5. basic requirements for training, drills and exercises in ship and company, port and port facility security;

1.6. requirements for cooperation and exchange of information between institutions involved in fulfilment of the requirements of ship and company, port and port facility security, and also the procedures for cooperation and exchange of information.

2. Within the meaning of this Regulation:

2.1. security requirements – requirements that are laid down in:

2.1.1. Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (hereinafter – Council Regulation No 725/2004);

2.1.2. Chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS) of 1974 with amendments (hereinafter – SOLAS Convention);

2.1.3. International Ship and Port Facility Security Code (hereinafter – ISPS Code);

2.1.4. this Regulation, Maritime Administration and Marine Safety Law, Law on Ports and laws and regulations regarding recognised security organisations in the field of shipping and port operation;

2.2. security information – the information referred to in Chapter XI-2, Regulation 9, Sub-paragraph 2.1 of the SOLAS Convention, provided by the ship prior to entry into a port;

2.3. security incident - an incident as defined in Chapter XI-2, Regulation 1, Sub-paragraph 1.13 of the SOLAS Convention;

2.4. recognised security organisation – an organisation as defined in Chapter XI-2, Regulation 1, Paragraph 16 of the SOLAS Convention;

2.5. ship security officer – the person on board the ship, accountable to the master, designated by the company as responsible for the security of the ship, including implementation and maintenance of the ship security plan, and for liaison with the company security officer and port facility security officer;

2.6. ship to ship activity – any activity not related to a port facility and that involves the transfer of goods or persons from one ship to another;

2.7. ship and port interface – a process 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 the ship;

2.8. company – a ship owner or any other legal or natural person (such as the ship operator or the bareboat charterer), who has assumed the duties and responsibility for operation of the ship from the ship owner, including all the duties and liability imposed by the International Management Code for the Safe Operation of Ships and for Pollution Prevention (*ISM* Code);

2.9. company security officer – the person designated by the company for ensuring that a ship security assessment is carried out, that a ship security plan is developed, submitted for approval and thereafter implemented and maintained, and for liaison with port facility security officer and the ship security officer;

2.10. focal point for ship and port security – an authority which in accordance with Council Regulation No 725/2004 and this Regulation:

2.10.1. acts as a contact point for international institutions and foreign competent institutions in the field of port and port facility security;

2.10.2. facilitates and monitors application of security requirements;

2.10.3. provides information on application of security requirements. The focal points for ship and port security in Latvia are as follows: the Maritime Administration and the Search and Rescue Coordination Centre of the Coast Guard Service of the National Armed Force Naval Forces Flotilla (MRCC RIGA) (hereinafter – the Coast Guard);

2.11. national SSN system – a vessel traffic monitoring and information data exchange system in accordance with the laws and regulations regarding vessel traffic monitoring and information data exchange system;

2.12. port – a territory of the port of Latvia or a section of the port territory with at least one port facility whereto the port facility security plan is applicable;

2.13. port security authority - an authority laid down in Paragraph 167 of this Regulation and responsible for security matters at the port;

2.14. port facility - a place where the ship and port interface takes place, and which in conformity with the security assessment is established by the SPSI. Depending on a specific case, it may include anchorages, awaiting berths and access to them from the sea;

2.15. port facility security officer – 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 officer and company security officer;

2.16. owner or possessor of the port facility – a person owing or possessing the port facility or acting on behalf of the owner or possessor;

2.17. justified reasons – the reasons for performing an inspection of the ship as defined in Part B, Sub-paragraph 4.33 of the ISPS Code;

2.18. scheduled voyages - the voyages as defined in Article 2, Paragraph 10 of Council Regulation No 725/2004.

3. Ship and company, port and port facility security functions laid down in the laws and regulations referred to in Sub-paragraph 2.1 of this Regulation shall be performed by the Maritime Administration, the Naval Forces Flotilla of the National Armed Forces, the Security Police, the State Border Guard, the customs authorities of the State Revenue Service, the recognised security organisations and port authorities.

4. Requirements of this Regulation shall be applicable to:

4.1. the ships laid down in Part A, Sub-paragraph 3.1.1 of the ISPS Code, taking into account Part A, Sub-paragraph 3.3 of the ISPS Code;

4.2. port facilities (except for military port facilities) laid down in Part A, Sub-paragraph 3.1.2 of the ISPS Code, and having interaction with the ships referred to in Sub-paragraph 4.1 of this Regulation;

4.3. ships engaged in domestic voyages:

4.3.1. if a ship conforms to the requirements for the passenger ships laid down in Article 3, Paragraph 2 of Council Regulation No 725/2004;

4.3.2. if a MSI inspector establishes that a failure to apply this Regulation would create significant threats to the relevant ship, its passengers, cargoes or the ports or port facilities related thereto;

4.4. ports;

4.5. territories adjacent to ports – in accordance with security assessment of the relevant port;

4.6. port facilities servicing the ships referred to in Sub-Paragraph 4.3 of this Regulation based on the port security assessment;

4.7. recognised security organisations.

5. In order to fulfil the obligations laid down by the Maritime Administration and ensure effective compliance with the security requirements, SPSI and MSI inspectors in accordance with the competence laid down in this Regulation have the right to:

5.1. carry out the ship security control measures in accordance with Chapter XI-2, Regulation 9 of the SOLAS Convention;

5.2. request from the designated authorities and persons to perform the ship, port and port facility security drills and exercises, provide instructions in respect of these drills and exercises and participate in the drills and exercises of ship, port and port facility security organised by other designated authorities;

5.3. provide recommendations on the planned measures for ensuring ship, port and port facility security in accordance with the security requirements;

5.4. by presenting a service pass, visit the ports of Latvia and territories adjacent thereto, port facilities, any ship on the territory within the jurisdiction of the Republic of Latvia and ships flying the flag of Latvia on the territories in the jurisdiction of other countries.

**2. Ship Security**

**2.1. General Description**

6. Implementation of the ship security requirements has the following stages:

6.1. ship security assessment;

6.2. preparation of the ship security plan (assessment and coordination), taking into account the security measures for each security level referred to in Part A, Sub-paragraphs 2.1.9, 2.1.10 and 2.1.11 of the ISPS Code;

6.3. approval of the ship security plan;

6.4. implementation of the security measures laid down in the ship security plan;

6.5. initial verification of ship security;

6.6. issuing of the International Ship Security Certificate or Interim International Ship Security Certificate.

7. In order to monitor compliance with the ship security requirements, the authorities referred to in Paragraph 3 of this Regulation pursuant to their competence shall perform:

7.1. verifications of ship security;

7.2. control measures of ship security in accordance with the requirements of Chapter XI-2, Sub-paragraph 9.1.3 of the SOLAS Convention;

7.3. analysis of the security information;

7.4. exchange of information with the authorities responsible for ship security, or persons interested in ship security.

**2.2. Ship Security Assessment**

8. Company security officer shall carry out the security assessment for the ships referred to in Sub-paragraph 4.1 of this Regulation.

9. MSI inspector shall carry out the security assessment for the ships referred to in Sub-paragraph 4.3 of this Regulation.

10. When assessing ship security, the officials referred to in Paragraphs 8 and 9 of this Regulation in accordance with Part A, Paragraph 8 and Part B, Paragraph 8 of the ISPS Code shall:

10.1. identify possible threats to the ship and likelihood of their occurrence, in order to establish security measures;

10.2. prepare the ship security assessment, providing recommendations and instructions on security measures to be included in the ship security plan, and establish and prioritize security measures (for example, provision of access control, establishment of restricted access areas, their monitoring, completion of security declarations).

11. The ship security assessment shall be prepared in the working language (languages) of the ship. If it is not English, a translation in English shall also be prepared. The company shall verify by documents that the translations of the ship security assessment in different languages are authentic.

12. In order to evaluate ship security and prepare an assessment, the company security officer may use services of a recognised security organisation pursuant to Part B, Paragraph 4.4 of the ISPS Code.

**2.3. Preparation and Approval of the Ship Security Plan and Amendments Thereto**

13. The ship security plan or any amendments thereto shall be prepared by the company security officer. The ship security plan or any amendments thereto may be developed by a recognised security organisation, taking into consideration the requirements of Part B, Paragraph 4.4 of the ISPS Code. The following information shall be used for the preparation of the ship security plan or amendments thereto:

13.1. the information included in the ship security assessment;

13.2. conclusions drawn by analysing the information included in the ship security assessment;

13.3. conclusions drawn by analysing the actual circumstances on the ship;

13.4. conclusions drawn by analysing the recommendations of the MSI and the authorities connected with State safety and security (for example, the State Police, the Security Police, the State Border Guard, the Naval Forces Flotilla of the National Armed Forces, the State Fire-fighting and Rescue Service).

14. The ship security plan or any amendments thereto shall be prepared in the working language (languages) of the ship. If it is not English, a translation in English shall also be prepared. The company shall verify by documents that the translations of the plan in different languages are authentic.

15. The ship security plan together with security assessment or amendments to the ship security plan with a submission regarding approval of the ship security plan or amendments thereto shall be submitted to the MSI.

16. A MSI inspector shall evaluate the conformity of the ship security plan and the relevant ship security assessment or amendments to the ship security plan to the security requirements.

17. If during an evaluation of the ship security plan or any amendments thereto the MSI inspector establishes non-conformities with the requirements referred to in Paragraph 16 of this Regulation, a person preparing the ship security plan at the instruction of the MSI inspector shall rectify the established deficiencies prior to taking a decision to approve the ship security plan or amendments thereto.

18. The ship security plan or amendments thereto shall be approved in three counterparts, making an appropriate approval note on the front pages of the submitted original ship security plan or amendments thereto in accordance with the requirements laid down in the laws and regulations regarding the procedures for developing and drawing up documents. After approval one counterpart of the approved plan or amendments thereto shall be kept by the MSI, while the other two are returned to the submitter.

19. After approval of the amendments to the ship security plan, the pages of the ship security plan wherein amendments were made shall be replaced, and a notation shall be made in the amendment registration sheet. Replaced pages with the old wording of the ship security plan shall be destroyed. The aforementioned actions shall be taken by:

19.1. the ship security officer – in the counterpart of the ship security plan stored on the ship;

19.2. the company security officer – in the counterpart of the ship security plan stored by the company.

20. In order to ensure conformity of the ship security plan with the existing security situation on the ship, the company or ship security officer shall review it in full at least once a year. The training, drills and exercise plans of the ship security personnel shall be reviewed at least once a year. Appropriate information shall be indicated in the section of the ship security plan laying down a need for regular revision and updating of the ship security plan.

21. The MSI does not need to approve minor amendments to the ship security plan (for example, changes in the contact information of company and ship security officer, changes to the training, drills and exercise plans of the ship security personnel, other minor amendments not significantly affecting the ship security system).

22. If any of the changes referred to in Paragraph 21 of this Regulation have taken place, the relevant amendments shall be made in the ship security plan, and information on the made amendments shall be provided to the MSI as soon as possible.

23. The ship security records referred to in Part A, Paragraph 10.1 of the ISPS Code after approval of the ship security plan shall be stored on the ship for three years, in compliance with the requirements of Chapter XI-2, Sub-paragraph 9.2.3 of the SOLAS Convention.

**2.4. Verifications of Ship Security**

24. In order to verify conformity of the ship security system with the ship security requirements, a MSI inspector shall perform verifications of ship security. The verifications of ship security may also be performed by a recognised security organisation, if it has obtained a permit from the Maritime Administration. The abovementioned permit shall be issued for one verification.

25. A MSI inspector may perform the security verification of any ship in the territory of the jurisdiction of the Republic of Latvia. The inspector may perform the security verification of the ship flying the flag of Latvia also in the territory of the jurisdiction of other countries. The inspector is entitled to demand a ship to go to a certain place of the port or in sea, or not to leave this place, in order to be able to perform its security verification.

26. MSI inspector shall perform the following verifications of the ship security:

26.1. initial verification – a verification performed before issuing of the International Ship Security Certificate or Interim International Ship Security Certificate;

26.2. intermediate verification – a verification performed during the period between the second and third year after issuing of the International Ship Security Certificate;

26.3. renewal verification – a verification performed before reissuance of the International Ship Security Certificate;

26.4. additional verification – a verification performed to verify constant conformity of the security system with the security requirements, as well as a verification performed based on the information received from other State authorities or legal or natural persons, or authorities of another country, if they have a justified reason to believe that the ship does not conform to security requirements.

27. If deficiencies in the ship security system not significantly reducing security of the ship (security is significantly reduced if the security system is unable to ensure constant complex security of people, ships and other property in the entire object) are established during any of the verifications referred to in Paragraph 26 of this Regulation, a reverification of the ship may be performed to verify that the deficiencies established during the previous verifications are rectified and other deficiencies have not appeared.

28. A MSI inspector shall perform a verification of the ship security based on a submission of the company, except for the additional verification. After receiving of a submission, the MSI inspector shall agree with the company regarding the time and place of the verification of the ship security system.

29. A verification of the ship security shall be performed within one day, but if the work load is high (verification may not be performed within one day), time of the verification may be extended for up to two working days.

30. A report shall be drawn up regarding results of the verification of the ship security, containing information regarding the ship, type of verification, established deficiencies with an indication of the infringed requirements. The report shall be signed by a person preparing it and a representative of the company. A representative of the company has the right to submit comments regarding the content of the report and specify the reasons for his or her refusal to sign it. The comments shall be added to the report.

31. If the results of the initial or renewal verification confirm the conformity of the ship security system to the ship security plan, the MSI inspector shall take a decision to issue the International Ship Security Certificate to the ship.

32. If conformity of the ship to the security requirements is established during any verification referred to in Paragraph 31 of this Regulation, but some deficiencies not significantly reducing the security are discovered, the MSI inspector shall take a decision to issue the International Security Certificate, where taking into account the opinion of the representative of the company to the extent possible a deadline (not later than one month after taking such decision) shall be indicated by which the established deficiencies are to be rectified. The company has an obligation to rectify the deficiencies referred to in the decision within the time period indicated by the inspector and notify the MSI thereof.

33. If the initial verification shows that the ship security system does not conform to the security requirements, the MSI inspector shall take a decision to refuse to issue the International Ship Security Certificate.

34. If the renewal verification shows that the ship security system does not conform to the security requirements, the MSI inspector shall take a decision to refuse to issue the International Ship Security Certificate and revoke the existing International Ship Security Certificate if the term of validity thereof has not yet expired.

35. If the results of the intermediate verification show conformity of the ship security system to the security requirements, the MSI inspector shall take a decision to make an approval note in the International Ship Security Certificate.

36. If the intermediate verification shows conformity of the ship to the security requirements, but deficiencies not significantly reducing security of the ship are established, the MSI inspector shall take a decision to make an endorsement of approval of the intermediate verification in the International Ship Security Certificate, and, by taking into consideration the opinion of the representative of the company to the extent possible, indicate a deadline for rectification of the established deficiencies. The company has an obligation to rectify the deficiencies referred to in the decision within the time period indicated by the MSI inspector and notify the MSI thereof.

37. If the intermediate verification shows that the ship security system does not conform to the security requirements, the MSI inspector shall take a decision to refuse to issue an approval note of the intermediate inspection in the International Ship Security Certificate and revoke the existing International Ship Security Certificate.

38. After an additional verification of the ship, the MSI inspector shall prepare a report and take one of the following decisions:

38.1. on conformity of the ship to the security requirements if the ship security system conforms to security requirements;

38.2. on conformity of the ship to security requirements with a task to rectify deficiencies established during the verification not significantly reducing security of the ship, and taking into consideration the opinion of the representative of the company to the extent possible, indicating a deadline for rectification of these deficiencies. The company has a duty to rectify the deficiencies referred to in the decision by the deadline indicated by the inspector and notify the MSI thereof;

38.3 on non-conformity of the ship to the security requirements and revocation of the ship security certificate, if the security system of the ship does not conform to security requirements.

39. The term of validity of the International Ship Security Certificate or Interim International Ship Security Certificate may be verified also by the following authorities:

39.1. the Naval Forces Flotilla of the National Armed Forces – by performing verification of the ship in accordance with its competence;

39.2. the State Border Guard – by performing verification of the ship in accordance with its competence;

39.3. Customs authorities of the State Revenue Service – by performing verification of the ship in the scope of the customs supervision.

**2.5. International Ship Security Certificate**

40. International Ship Security Certificate (Annex 1) is issued by the MSI after the verification referred to in Sub-paragraph 26.1 or 26.3 of this Regulation. The International Ship Security Certificate based on Section 13, Paragraph one of the Maritime Administration and Marine Safety Law may be issued also by a recognised security organisation, if such authorisation is provided for in the agency agreement signed between the Maritime Administration and a recognised security organisation.

41. The MSI may issue the International Ship Security Certificate by not performing the verification referred to in Sub-paragraph 26.1 or 26.3 of this Regulation, if the MSI has been submitted a summary of the ship security audit performed by an authorised recognised security organisation, as well as a Statement of Compliance or an Interim International Ship Security Certificate issued by the abovementioned organisation, verifying conformity of the relevant ship with the security requirements.

42. An International Ship Security Certificate may be issued by the MSI also to a ship flying the flag of another country, if a competent authority of this country has expressed such request in writing, and the MSI has been provided with an approved ship security plan and ship security assessment.

43. The MSI shall, within five working days from the receipt of the documents referred to in Paragraph 41 or 42 of this Regulation and taking a decision referred to in Paragraph 31 or 32 of this Regulation, issue the International Ship Security Certificate.

44. The International Ship Security Certificate is issued for a period up to five years. The International Ship Security Certificate may be issued for a period shorter than five years if:

44.1. The MSI has in its possession information regarding a planned change of the actual circumstances in respect of the ship during the period of time which is shorter than five years from issuing of the certificate (for example, reconstruction or termination of the operation of the ship, change of the ship security system, change of the ship owner or possessor is planned);

44.2. a relevant written request is received from the company.

45. If a name or type of the ship or a legal address of the company changes during the term of validity of the International Ship Security Certificate, the company shall, within three working days after these changes taking place, submit an application to the MSI for issuing of a new International Ship Security Certificate. Based on the received submission and results of the verifications of ship security performed for issuing of the previous certificate, the MSI shall, within three working days after the receipt of the submission, take a decision to issue a new International Ship Security Certificate. It shall be issued for a period not exceeding the term of validity of the initial interim certificate.

46. If the International Ship Security Certificate is damaged, lost or stolen, the company shall immediately inform the MSI thereof.

47. A new International Ship Security Certificate, if the term of validity of the existing certificate has expired, shall be issued by the MSI after the verification referred to in Sub-paragraph 26.3 of this Regulation.

48. A MSI inspector may extend the term of validity of the International Ship Security Certificate, change it or recognise the International Ship Security Certificate with the expired term of validity as valid in accordance with Part A, Sub-paragraph 19.3.3, 19.3.4, 19.3.5, 19.3.6 or 19.3.7 of the ISPS Code, by making a note thereon in the certificate or notifying thereof to the company in conformity to the Law on Notification.

**2.6. Interim International Ship Security Certificate**

49. The MSI may issue an Interim International Ship Security Certificate (Annex 2), if:

49.1. the ship does not have any international ship security certificate, during delivery of the ship or prior to putting into operation or repeated putting into operation thereof;

49.2. the ship is being re-registered from the ship register of another country into the Ship Register of Latvia;

49.3. the company of the ship has changed.

50. For receipt of the Interim International Ship Security Certificate, the company shall submit the following information to the MSI:

50.1. ship security assessment;

50.2. the existing ship security plan that is implemented on the ship and conforming to the requirements of Chapter XI-2 of the SOLAS Convention and Part A of the ISPS Code;

50.3. documents which attest that training, drills and exercises have been carried out pursuant to security requirements (ship personnel knows its obligations in accordance with the ship security plan);

50.4. documents which attest that a security alarm system of the ship is installed and operates on the ship in accordance with the requirements of the laws and regulations regarding ensuring the operation of the communication network of the ship security alarm signals;

50.5. a certificate of the ship security officer;

50.6. copies of the previously issued International Ship Security Certificates or Interim International Ship Security Certificates, if such were issued for the particular ship;

50.7. report of internal audit of the ship security performed by the company security officer in the cases referred to in Paragraph 49 of this Regulation;

50.8 other information in accordance with Part A, Sub-paragraph 19.4.2 of the ISPS Code – at the request of the MSI inspector.

51. The MSI inspector shall, within three working days from the receipt of the documents referred to in Paragraph 50 of this Regulation, take a decision to issue an Interim International Ship Security Certificate or to refuse to issue the Interim International Ship Security Certificate.

52. If the company is unable to submit the documents referred to in Paragraph 50 of this Regulation, or if the submitted documents indicate non-conformity of the ship to the security requirements, or they do not allow to verify the conformity of the ship to these requirements, the MSI may issue an Interim International Ship Security Certificate only after the initial verification of ship security.

53. The Interim International Ship Security Certificate shall be issued for a period of six months. It shall be valid for six months or until the moment when an International Ship Security Certificate is issued to the ship.

54. If a name or type of the ship or a legal address of the company changes during the term of validity of the Interim International Ship Security Certificate, the company shall, within three working days after these changes taking place, submit an application to the MSI for issuing of a repeated Interim International Ship Security Certificate. Based on the received submission and the results of the verifications of ship security performed for issuing of the previous certificate, the MSI shall, within three working days after the receipt of the submission, take a decision to issue a repeated Interim International Ship Security Certificate. It shall be issued for a period not exceeding the term of validity of the initial interim certificate.

55. If the Interim International Ship Security Certificate is damaged, lost or stolen, the company shall immediately inform the MSI thereof.

56. The Interim International Ship Security Certificate based on Section 13, Paragraph one of the Maritime Administration and Marine Safety Law may be issued also by a recognised security organisation, if such authorisation is provided for in the agency agreement signed between the Maritime Administration and the recognised security organisation.

57. The MSI shall take a decision to revoke the Interim International Ship Security Certificate if non-conformity of the ship security system to the security requirements is established during the verification of ship security.

**2.7. Security Control Measures in Respect of Foreign Ships**

58. In order to verify constant conformity of the security system to the security requirements, the SPSI inspector shall perform a security verification of the foreign ship prior to entering a port of Latvia or while being in a port of Latvia.

59. The SPSI inspector is entitled to detain a ship in order to perform its verification of ship security.

60. If non-conformity of the ship security system to the security requirements is established during the verification of the ship security, and people, ships or other property is significantly endangered as the result thereof, the SPSI inspector may take a decision to deny an entry of the ship into a port, to detain the ship, to suspend operations of the ship, to prohibit the ship to move around the port or to expel the ship from the port. A decision to prohibit the ship to enter the port or to expel the ship from the port may be taken by the SPSI inspector only if there are justified grounds to think that this ship directly endangers persons, ships or other property, and if other appropriate means to prevent such danger do not exist.

61. A decision to detain the ship, to suspend operations of the ship, to prohibit the ship to move around the port or release of the ship shall be enforced by the captain of the port where the ship is located, while a decision to expel the ship from the port – by the Coast Guard. In order to ensure enforcement of the abovementioned decisions, the Maritime Administration shall send the relevant decision to the captain of the port and Coast Guard. The Coast Guard shall, after receipt of the decision, make an appropriate endorsement in the national SSN system.

62. The Coast Guard shall, in a timely manner (immediately after taking the decision to expel the ship), inform the authorities referred to in Sub-paragraphs 81.2, 81.3 and 81.4 of this Regulation regarding the decision made by the Maritime Administration to expel the ship from the port.

63. If the ship is detained, expelled from the port or operations of the ship are suspended, the Maritime Administration shall immediately issue the relevant notice to the master of the ship.

64. After rectification of all deficiencies established during the verification on the ship which was detained or the operations whereof were suspended, the master of the ship shall notify the Marine Administration thereof, so that a reverification of the ship security may be performed.

65. If after security reverification referred to in Paragraph 64 of this Regulation, the SPSI inspector establishes that the ship may navigate in the port, navigate into the sea or resume the operations of the ship, the SPSI inspector shall withdraw the relevant prohibition.

66. By withdrawing the prohibitions referred to in Paragraph 65 of this Regulation, the SPSI inspector shall complete a notification regarding withdrawal of the ship prohibition and inform the Coast Guard, which makes a relevant endorsement in the national SSN system. A notification shall be issued to the master of the ship, while a copy of the notification – to the master of the relevant port or the Coast Guard (depending on who enforces the relevant decision), flag country of the ship and recognised security organisation issuing the International Ship Security Certificate or Interim International Ship Security Certificate.

67. Prior to a ship entering the port of Latvia, the Coast Guard during analysis of the security information after consultation with the authorities referred to in Paragraph 81 of this Regulation in accordance with their competence may:

67.1. request to rectify deficiencies in the ship security system;

67.2. request the ship to go to the indicated location;

67.3. request to perform the verification of the ship security;

67.4. place a prohibition for the ship to enter the port.

68. The verification of the ship security referred to in Sub-paragraph 67.3 of this Regulation upon request of the Coast Guard shall be performed by the SPSI inspector prior to the entering the port by the ship. If the SPSI inspector has justified grounds to believe that the ship does not conform to security requirements, it shall take a decision to prohibit the ship to enter the port until the moment when non-conformity to security requirements is rectified.

69. The Coast Guard may apply the measures referred to in Paragraph 67 of this Regulation without consulting the authorities referred to in Paragraph 81 of this Regulation, if consulting is impossible due to objective reasons (for example, urgency, emergency situation in the country, etc.).

70. Prior to commencement of the measures referred to in Paragraph 67 of this Regulation, the Coast Guard shall immediately inform the master of the relevant ship. The Coast Guard shall also inform the authorities referred to in Paragraph 81 of this Regulation regarding the taken decision.

71. If the ship in accordance with the laws and regulations regarding the procedures for use of the waterways of Latvia and navigation regime is granted a place of refuge in a port of Latvia, the Maritime Administration may not prohibit the ship to enter the port of refuge, but a security verification thereof shall be performed by the SPSI inspector after the ship has entered the port of refuge.

72. In order to withdraw a prohibition to enter the port, the SPSI inspector shall perform a reverification of the ship security to verify its conformity with the security requirements.

73. The Coast Guard shall perform the functions of the competent authority referred to in Chapter XI-2, Regulation 4, Paragraph 5 of the SOLAS Convention.

74. The Naval Forces Flotilla of the National Armed Forces shall ensure enforcement of the decision to prohibit to enter the port or to expel from the port.

75. If a ship is prohibited to enter the port, or the ship is expelled from the port, the Maritime Administration shall, as soon as possible, inform also the International Maritime Organisation, the European Commission, other European Union Member States and the relevant country of the flag. The SPSI shall send the abovementioned information also to the recognised security organisation which has issued the International Ship Security Certificate or Interim International Ship Security Certificate.

**2.8. Security Information**

76. The ship planning to enter a port of Latvia shall provide security information in accordance with the procedures laid down in the laws and regulations regarding port formalities.

77. The Coast Guard shall, in cooperation with the Security Police and Maritime Administration, evaluate the received security information and exchange the additional information in their possession which is to be taken into account during the security assessment process of the relevant ship.

78. Once the ship has submitted security information in accordance with Paragraph 76 of this Regulation, the Coast Guard shall verify whether the relevant ship has a valid International Ship Security Certificate or Interim International Ship Security Certificate, and the port facility, at which the ship is planning to dock, has a valid Statement of Security Compliance of the Port Facility and, where such exists, – whether security level of the ship conforms to security level of the relevant port facility.

79. The Coast Guard shall inform the ship, port, port section or port facility operating at a lower security level regarding a necessity to enhance security measures, as well as inform the Security Police, if:

79.1. after the verification of information referred to in Paragraph 76 of this Regulation, the Coast Guard determines that the ship does not have a valid ship security certificate or the port facility lacks a valid Statement of Security Compliance or that the security levels of the ship and port facility do not coincide;

79.2. information is received from a ship that the ship which is preparing to be re-moored, or a port facility to which a ship is preparing to be re-moored, does not have a valid Statement of Security Compliance or that the security levels of the ship and port facility do not coincide.

80. If after the verification of the information referred to in Paragraph 76 of this Regulation, the Coast Guard determines that the ship does not have a valid ship security certificate or the port facility lacks a valid Statement of Security Compliance, or that the security levels of the ship and port facility do not coincide, the Coast Guard shall inform the ship, port, part of the port or port facility thereof, wherewith the interface is planned.

81. If the Coast Guard after analysis of the security information establishes that the ship does not conform to security requirements, or justified suspicions exist regarding its conformity to security requirements, the Coast Guard shall notify the following authorities thereof:

81.1. the SPSI;

81.2. the Security Police;

81.3. the State Border Guard;

81.4. the customs authority of the State Revenue Service.

82. Control measures may be applied in the situations referred to in Paragraph 81 of this Regulation in accordance with Paragraph 67 of this Regulation.

83. If the Coast Guard establishes that the ship has not provided security information, it shall act in accordance with Paragraph 81 of this Regulation, and inform the MSI regarding the fact of failure to provide information for it to be able to take appropriate measures in accordance with the laws and regulations regarding procedures for the port State control.

84. The Coast Guard shall, in accordance with Article 6 (3) of Council Regulation No 725/2004, prepare a report on compliance with the procedures for provision of the security information in respect of each ship where a security incident has taken place.

85. The Maritime Administration may exempt the ship from an obligation to provide the security information in conformity with the laws and regulations regarding the port formalities.

86. The company wishing to receive a waiver of the obligation to provide security information shall submit an application to the Maritime Administration, listing the following information:

86.1. ships performing the relevant scheduled voyages;

86.2. information regarding between which port facilities the relevant voyages take place;

86. 3 information attesting regularity of the relevant voyages;

86.4. information attesting creation of an internal system in the company ensuring that the security information is constantly available and may be sent to the Coast Guard immediately after its request.

87. The Maritime Administration shall evaluate the information submitted in accordance with Paragraph 86 of this Regulation and take a decision to exempt the ship from the obligation to provide security information – if its voyages conform to the information referred to in Article 7 (1) of Council Regulation No 725/2004, and exemption from the obligation to provide security information would not endanger security of the objects referred to in Sub-paragraph 4.1, 4.4 or 4.6 of this Regulation.

88. The company, the ships whereof are exempted from the obligation to provide security information in accordance with Paragraph 85 of this Regulation shall:

88.1. immediately inform the Maritime Administration regarding any changes to the information provided in accordance with Paragraph 86 of this Regulation;

88.2. ensure a 24-hour option of sending security information on each voyage made by the relevant ship immediately after a request made by the Coast Guard.

89. The Maritime Administration in accordance with the information referred to in Article 7(3) of Council Regulation No 725/2004 shall take a decision to revoke an exemption granted in accordance with Paragraph 85 of this Regulation if:

89.1. any of the conditions based on which the exemption was granted is not complied with;

89.2. the company fails to fulfil the obligations referred to in Paragraph 88 of this Regulation.

90. The Coast Guard shall inform the ship, port, port section or port facility regarding the security level laid down for this ship, port, port section or port facility in accordance with Paragraph 212 of this Regulation, and that the ship, port, port section or port facility wherewith interface is anticipated, does not have a valid Statement of Security Compliance.

**3. Port Facility Security**

**3.1. General Description**

91. Implementation of the port facility security requirements has the following stages:

91.1. port facility security assessment;

91.2. approval of the port facility security officer;

91.3. preparation of the port facility security plan;

91.4. approval of the port facility security plan;

91.5. implementation of the security measures laid down in the port facility security plan;

91.6. initial verification of the port facility security;

91.7. issuing the Statement of Security Compliance of the Port Facility.

92. In addition to the information referred to in Paragraph 91 of this Regulation, the port facility security requirements shall be implemented taking into account the security level referred to in Part A, Sub-paragraphs 2.1.9, 2.1.10 and 2.1.11 of the ISPS Code.

93. In order to monitor compliance with the port facility security requirements, the SPSI inspector shall perform the security verification of the port facility and coordination of the training programmes of the port facility security personnel, as well as he or she is entitled to request and receive the information related to the port facility security.

**3.2. Port Facility Security Assessment**

94. The owner or possessor of the port facility in accordance with the requirements of this Regulation shall organise the security assessment of the port facilities servicing the ships referred to in Sub-paragraph 4.1 or 4.3 of this Regulation, by submitting an application to the SPSI for the port facility security assessment.

95. The SPSI shall evaluate the port facility referred to in Paragraph 94 of this Regulation and determine if security requirements are applicable thereto, taking in to consideration Article 3(3) of Council Regulation 725/2004 and Chapter XI-2, Regulation 2, Paragraph 2 of the SOLAS Convention.

96. The port facility security assessment shall be performed by the SPSI inspector in compliance with the conditions of Part A, Paragraph 15 and Part B, Paragraph 15 of the ISPS Code.

97. In order to evaluate the port facility security, the SPSI inspector shall gather the information regarding the port facility, and send to the owner or possessor of the port facility a security assessment questionnaire with questions related to the port facility security and risk, and carry out assessment of the port facility, by coordinating it with the owner or possessor of the port facility in advance.

98. The owner or possessor of the port facility shall submit a completed security assessment questionnaire to the SPSI not later than within three working days prior to assessment of the port facility.

99. The SPSI inspector shall prepare a port facility security assessment, including in it the information based on the elements of the port facility security assessment referred to in Part A, Sub-paragraphs 15.5, 15.7 and Part B, Sub-paragraph 15.3 of the ISPS Code, and submit it for the approval to the Director of the Maritime Safety Department of the Maritime Administration.

100. Port facility security assessment shall be prepared in three counterparts, and within 15 days after the assessment of the port facility one counterpart of the port facility security assessment shall be sent to the owner or possessor of the port facility, the second – to the port security authority, while the third shall be kept by the SPSI.

101. The SPSI inspector shall issue recommendations and instructions on security measures to be included in the port facility security plan in respect of the port facilities referred to in Paragraph 95 of this Regulation, by indicating priority security measures (for example, ensuring of access control, designation of restricted access areas, their monitoring, preparation of security declarations), and determine a reasonable deadline for submission of the plan to the SPSI.

102. If any changes to the port facility or risks thereto have taken place, the owner or possessor of the port facility has an obligation to immediately provide the relevant information to the SPSI. Based on the this current information regarding changes to the port facility or risks thereto, the SPSI inspector shall evaluate the port facility security and, where necessary, make amendments to the port facility security assessment. Amendments shall be approved by the Director of the Maritime Security Department.

103. The SPSI inspector shall, within five working days, inform the owner or possessor of the port facility regarding results of the port facility security assessment.

104. The SPSI inspector shall perform the port facility security assessment at least once in five years.

3.3. Port facility security officer

105. The SPSI at the written request of the owner or possessor of the port facility shall approve a port facility security officer for each port facility.

106. A candidate for the port facility security officer proposed by the owner or possessor of the port facility shall be approved if he or she conforms to the requirements laid down for the port facility security officer in Part A, Sub-paragraph 18.1 of the ISPS Code.

107. If the SPSI establishes that the approved port facility security officer does not any longer conforms to the requirements laid down in Paragraph 106 of this Regulation, it may take a decision to revoke the approval of the port facility security officer and request the owner or possessor of the port facility to propose another candidate for the port facility security officer.

108. One port facility security officer may be approved for several port facilities within the scope of one port.

109. The port facility security officer shall perform the duties related to port facility security in accordance with the duties for the port facility security officer laid down in Part A, Paragraphs 17 and 18 of the ISPS Code, and shall be a contact person in the matters related to port security.

110. If the port facility security officer is not at the same time also a port security officer, the port facility security officer shall cooperate with the port security officer of the relevant port.

111. The port facility security officer may be replaced only by a person conforming to the requirements laid down for the port facility security officer in Part A, Sub-paragraph 18.1 of the ISPS Code. The SPSI shall not separately approve this person, and his or her conformity to the requirements laid down in this Paragraph shall be verified by the SPSI during the port facility security inspections.

**3.4. Preparation and Approval of the Port Facility Security Plan and Amendments Thereto**

112. The port facility security plan or any amendments thereto shall be prepared by the port facility security officer. The port facility security plan or any amendments thereto may be prepared by a recognised security organisation, taking into consideration the requirements of Part B, Sub-paragraph 4.4 of the ISPS code. The port facility security plan or any amendments thereto shall be prepared in compliance with the following terms and conditions:

112.1. the port facility security plan shall be prepared in accordance with the structure of the plan laid down in Annex 3 to this Regulation;

112.2. the following information shall be used for the preparation of the port facility security plan or amendments thereto:

112.2.1. the information included in the port facility security assessment;

112.2.2. conclusions drawn by analysing the information included in the port facility security assessment;

112.2.3. conclusions drawn by analysing the actual circumstances in the port facility;

112.2.4. conclusions drawn by analysing the recommendations made by the SPSI and the institutions related to State security (for example, the State Police, the Security Police, the State Border Guard, the Naval Forces Flotilla of the National Armed Forces, the State Fire-fighting and Rescue Service);

112.2.5. Assessment performed by the Security Police of the information submitted by the SPSI regarding the current risk assessment for the port facility, if any is requested;

112.3. port facility security plan or amendments thereto shall be prepared in Latvian.

113. The port facility security plan or amendments thereto together with an application for approval of the port security plan or amendments thereto shall be submitted to the SPSI.

114. A SPSI inspector shall evaluate conformity of the port facility security plan or amendments thereto to the security requirements, as well as conformity of their appearance to the laws and regulations regarding procedures for developing and drawing up the documents.

115. If during evaluation of the port facility security plan or any amendments thereto the SPSI inspector establishes non-conformities with the requirements referred to in Paragraph 114 of this Regulation, the person preparing the port facility security plan shall, at the instruction of the SPSI inspector, eliminate the established deficiencies prior to taking a decision to approve the port facility security plan or amendments thereto.

116. The port facility security plan or amendments thereto shall be approved in three counterparts, making an appropriate approval note on the front pages of the submitted original port facility security plan or amendments thereto in accordance with the requirements laid down in the laws and regulations regarding procedures for developing and drawing up the documents. After approval, one counterpart of the approved plan or amendments thereto shall be sent by the SPSI to the owner or possessor of the port facility, the second – to the port security authority, while the third original counterpart shall be kept by the SPSI.

117. After approval of amendments to the port facility security plan, the port facility security officer shall ensure that the port facility security plan is accordingly updated, by changing those pages of the plan where the amendments were made, and making a relevant notation in the amendment recording sheet. The replaced pages with the old wording of the security plan shall be destroyed.

118. In order to ensure conformity of the port facility security plan with the existing security situation of the port facility, the port facility security officer shall review it in full at least once in six months. The training, drills and exercise programme of the port facility security personnel shall be prepared for the next year and submitted to the SPSI by 1 December of the current year. Appropriate information shall be indicated in the section of the port facility security plan laying down a need for a regular revision and updating the port facility security plan.

119. The SPSI does not need to approve minor amendments to the port facility security plan (for example, changes in the contact information of the port facility and port facility security officer, changes to the training, drills and exercise plans of the port facility security personnel, other minor amendments not significantly affecting the port facility security system).

120. If any changes referred to in Paragraph 119 of this Regulation have taken place, the relevant amendments shall be made in the port facility security plan, and information on the made amendments shall be provided to the SPSI as soon as possible.

**3.5. Storing of the Port Facility Security Plan, Amendments Thereto, and Port Facility Security Records**

121. The parts of the port facility security plan, draft plan, amendments and draft amendments, as well as the parts of the port facility security records shall be assigned a status “information for service purposes” and provided with appropriate security in accordance with the Freedom of Information Law and laws and regulations regarding the procedures for protection of information for the service needs.

122. The port security records shall be at least:

122.1. summaries of the port facility security training, drills and exercises;

122.2. records of the port facility security incidents and risks;

122.3. records of the infringements in the area of port facility security;

122.4. records of the change of port facility security levels;

122.5. records on inspections, maintenance and calibration of the port facility security equipment;

122.6. records of the implementation of the amendments to port facility security plan;

122.7. recording of verifications of the port facility security system;

122.8. records of the revision of the port facility security plan;

122.9. records of the revision of the port facility security assessment;

122.10. security declarations;

122.11. records of the risk to the ship or port facilities, where the ship is located or has been located.

123. One approved counterpart of the port facility security plan and a counterpart of amendments thereto shall be stored in the port facility, the second counterpart – in the port, while the third counterpart – by the SPSI.

124. Security records of the port facility shall be stored in the port facility for at least five years.

**3.6. Verification of Port Facility Security**

125. In order to verify the conformity of the port facility security system with the security requirements for the port facility, a SPSI inspector shall perform the security verifications of the port facility.

126. The SPSI inspector shall perform the following verifications of the port facility security:

126.1. initial verification – a verification performed at the beginning of operation of the port facility;

126.2. annual verification – a verification performed once a year after issuing the Statement of Security Compliance of the Port Facility in order to regularly verify conformity of the port facility with the security requirements (period between the inspections shall not be less than 10 months and shall not exceed 12 months);

126.3. renewal verification – a verification performed once in five years prior to reissuance of the Statement of Security Compliance of the Port Facility to the relevant port facility;

126.4. additional verification – any verification other than verification referred to in Sub-paragraph 126.1, 126.2 or 126.3 of this Regulation and performed by the SPSI inspector to verify constant conformity of the security system to the security requirements, as well as a verification performed based on the information received from other authorities related to State security (for example, the State Police, the Security Police, the State Border Guard, the Naval Force of the National Armed Forces, the State Fire-fighting and Rescue Service) or other legal or natural persons, regarding non-conformity of the port facility to the security requirements.

127. If deficiencies in the port facility security system not significantly reducing security of the port facility are established during any of the verification referred to in Paragraph 126 of this Regulation, a reverification of the port facility shall be performed to verify that the deficiencies established during the previous inspection are rectified and other deficiencies have not appeared. The port facility security significantly decreases if the security system is unable to ensure constant complex security of people, ships and other property in the entire object, for example, access control is not provided, designation of restricted access areas and their monitoring or preparation of security declarations is not ensured. If the deficiencies established during any of the inspections referred to in Sub-paragraphs 126.2, 126.3 or 126.4 of this Regulation are not rectified during a reverification, or new deficiencies have occurred, the SPSI shall take a decision to revoke the Statement of Security Compliance of the Port Facility.

128. A SPSI inspector shall perform a verification of the port facility security based on the submission of the owner or possessor of the port facility, except for the first additional verification.

129. A verification of the port facility security shall be performed within one day, but if the work load is high (verification may not be performed within one day), time of the verification may be extended up to two days.

130. A report shall be prepared regarding results of the verification of the port facility security (a deed of annual verification as a result of the verification referred to in Sub-paragraph 126.2 of this Regulation), providing in it the information regarding the port facility, type of verification, established deficiencies with a reference to the infringed security requirements, deadline for rectification of deficiencies and time of the next verification. The report shall be signed by a person preparing it and a representative of the port facility. If the representative of the port facility refuses to sign the report, an appropriate entry shall be made thereon in the report. A representative of the port facility or other persons ensuring the port facility security shall provide explanations on the deficiencies of the port facility security system established during verification. The abovementioned explanations shall be attached to the report. A representative of the port facility is entitled to submit comments regarding the content of the report and specify the reasons for his or her refusal to sign it. The comments shall be added to the report.

131. If the results of the initial or renewal verification confirm conformity of the port facility to the security requirements, the SPSI inspector shall take a decision to issue the Statement of Security Compliance of the Port Facility.

132. If conformity of the ship to the security requirements is established during any verification referred to in Paragraph 131 of this Regulation, but some deficiencies not significantly reducing the ship security are discovered, the SPSI inspector shall take a decision to issue the Statement of Security Compliance of the Port Facility and, by taking into account the opinion of the owner or possessor of the port facility to the extent possible, lay down a deadline (not later than two months after taking such decision) by which the provided deficiencies are to be rectified. The owner or possessor of the port facility has an obligation to rectify the deficiencies referred to in the decision by the deadline indicated by the SPSI inspector and notify him or her thereof.

133. If during any of the verification referred to in Paragraph 131 of this Regulation it is determined that the port facility security system does not conform to the security requirements, the SPSI inspector shall take a decision to refuse to issue the Statement of Security Compliance of the Port Facility and determine a deadline for the performance of a reverification. If a reverification is required, the Statement of Security Compliance of the Port Facility shall be issued after performance of the reverification. The owner or possessor of the port facility has an obligation to rectify the deficiencies referred to in the decision by the deadline indicated by the SPSI inspector.

134. If the results of the annual inspection confirm the conformity of the port facility to the security requirements, the SPSI inspector shall make an endorsement thereon in the Statement of Security Compliance of the Port Facility, by indicating the deadline in the deed of annual verification by which the next verification is to be performed.

135. If conformity of the port facility to the security requirements is established during an annual verification, but deficiencies not significantly reducing the port facility security are discovered, the SPSI inspector shall, to the extent possible taking into consideration the opinion of the owner or possessor of the port facility, indicate a deadline in the deed of annual verification (not later than two months after performance of verification) for rectification of the deficiencies established during the verification, and lay down a deadline for performance of a reverification. If a reverification is required, an endorsement shall be made in the Statement of Security Compliance of the Port Facility only after performance of the reverification. The owner or possessor of the port facility has an obligation to rectify the deficiencies referred to in the verification deed by the deadline indicated by the SPSI inspector.

136. If it is determined in the annual verification that the port facility security system does not conform to the security requirements, the SPSI inspector shall take a decision to revoke the Statement of Security Compliance of the Port Facility.

137. After additional verification of the port facility, the SPSI inspector shall prepare a report referred to in Paragraph 130 of this Regulation and take one of the following decisions:

137.1. regarding conformity of the port facility to the security requirements if the port facility conforms to security requirements;

137.2. regarding conformity of the port facility to security requirements with a task to rectify the deficiencies established during the inspection, which do not significantly reduce the port facility security, and, to the extent possible taking into account the opinion of the owner or possessor of the port facility, indicate the deadline (not later than two months after taking of such decision) for rectification of these deficiencies, and determine a deadline for a reverification. The owner or possessor of the port facility has an obligation to rectify the deficiencies referred to in the decision by the deadline indicated by the SPSI inspector;

137.3 regarding non-conformity of the port facility to security requirements and revocation of the Statement of Security Compliance of the Port Facility (if any issued), if the port facility does not conform to security requirements.

138. A SPSI inspector shall, during the verification of the port facility security, verify conformity of the port facility security system to the port facility security requirements.

139. If non-conformity of the port facility security system to the security requirements is established during the port facility security inspection, and people, ships or other property is endangered due to it, as well as any other appropriate means for rectification of this danger do not exist, the SPSI inspector may suspend operations in the port facility and request to rectify deficiencies in the security system. A decision to suspend operations shall, within one working day, be sent in writing to the person whereto the decision is applicable, as well as the master of the port who controls enforcement of such decision. The decision to suspend operations in the port facility shall be withdrawn only after a reverification if it is established that the deficiencies, due to which the operations were suspended, are rectified. A deadline (not later than two months after taking such decision) by which the deficiencies referred to in the decision are to be rectified shall be indicated in the decision to suspend operations, by indicating that the Statement of Security Compliance of the Port Facility (if it has been issued to the respective port) will be revoked, if the deadline is not complied with.

140. If the SPSI inspector establishes non-conformities to the security requirements in the port facility which in accordance with the laws and regulations regarding identification of critical infrastructure is included in the aggregation of the critical infrastructure, serving as the grounds for revocation of the approval of port facility security plan or amendments thereto, the SPSI shall immediately inform the Security Police.

**3.7. Statement of Security Compliance of the Port Facility**

141. Statement of Security Compliance of the Port Facility (Annex 4) shall be issued by the SPSI after performance of the verification referred to in Sub-paragraph 126.1 or 126.3 of this Regulation.

142. The SPSI shall, not later than within five working days after taking the decisions referred to in Paragraph 131 of this Regulation, issue a Statement of Security Compliance of the Port Facility to the owner or possessor of the port facility.

143. The Statement of Security Compliance of the Port Facility shall be issued for a period up to five years. The Statement of Security Compliance of the Port Facility may be issued for a period shorter than five years if:

143.1. the SPSI has in its possession the information regarding the planned change of the actual circumstances in respect of the port facility during the period shorter than five years from issuing of Statement of Security Compliance (for example, reconstruction or termination of the operation of the port facility, change of the port facility security system, change of the port facility owner or possessor is planned);

143.2. the SPSI reissues a Statement in accordance with the requirements of this Regulation;

143.3. a relevant written request is received from the owner or possessor of the port facility.

144. If the name, type of operation or legal address of the owner or possessor of the port facility is changed during the term of validity of the Statement of Security Compliance of the Port Facility, the owner or possessor of the port facility shall, within three working days after these changes, submit an application to the SPSI for issuing a new Statement of Security Compliance of the Port Facility. Based on the received submission and the results of the verifications of port facility security performed for issuing of the previous Statement, the SPSI shall, within three working days after the receipt of the submission, take a decision to issue a new Statement of Security Compliance of the Port Facility. It shall be issued for a period of time not exceeding the term of validity indicated in the previously issued Statement of Security Compliance.

145. If the Statement of Security Compliance of the Port Facility is damaged, lost or stolen, the owner or possessor of the port facility shall immediately notify the SPSI thereof.

146. The owner or possessor of the port facility shall submit the Statement of Security Compliance of the Port Facility, which is replaced by a new Statement of Security Compliance of the Port Facility in accordance with the requirements of this Regulation, or which was damaged, and a duplicate Statement of Security Compliance of the Port Facility is issued, or a term of validity of which has expired, to the SPSI within 14 working days after reissuance of the Statement of Security Compliance of the Port Facility, issue of the duplicate of the Statement or after expiry of the Statement.

147. A new Statement of Security Compliance of the Port Facility, if the term of validity thereof has expired, shall be issued by the SPSI after the verification referred to in Sub-paragraph 126.3 of this Regulation.

148. The Statement of Security Compliance of the Port Facility shall become invalid if the owner or possessor of the port facility has not ensured performance of the verification referred to in Sub-paragraph 126.2 of this Regulation by the deadline indicated by the SPSI.

**4. Port Security**

**4.1. General Description**

149. Implementation of the port security requirements has the following stages:

149.1. port security assessment and defining the boundaries of the protected territory;

149.2.appointment of the port security authority;

149.3. approval of the port security officer;

149.4. preparation of the port security plan;

149.5. approval of the port security plan;

149.6. implementation of the security measures laid down in the port security plan;

149.7. initial verification of the port security;

149.8. issuing the Statement of Security Compliance of the Port Facility.

150. In addition to the information referred to in Paragraph 149 of this Regulation, the port security requirements shall be implemented taking into account the security level indicated in Part A, Sub-paragraphs 2.1.9, 2.1.10 and 2.1.11 of the ISPS Code.

151. In order to monitor compliance with the port security requirements, a SPSI inspector shall perform the security verification of the port and coordination of the training programmes of the port security personnel, as well as he or she is entitled to request and receive the information related to the port security.

152. Security requirements laid down for the port shall be applicable to the port, unless it is otherwise provided for in this Regulation.

**4.2. Port Security Assessment and Defining Boundaries of Protected Territory of the Port**

153. Port security assessment in accordance with the requirements of this Regulation shall be organised by the port administration, by submitting a submission to the SPSI regarding performance of the port security assessment.

154. In order to evaluate port security, a SPSI inspector shall gather the information regarding the port, and send to the port administration a security assessment questionnaire with questions related to port security and risk, and carry out assessment of the port.

155. Not later than five working days prior to assessment of the port, a SPSI inspector shall notify the port authority thereof.

156. The port authority shall submit a completed security assessment questionnaire to the SPSI not later than within three working days prior to assessment of the port.

157. In order to define the boundaries of the port territory, where security measures are to be applied (hereinafter – protected territory), a SPSI inspector shall assess:

157.1. security of each port;

157.2. security of the territory adjacent to the port, if its insufficient security may cause risk to security of the objects referred to in Sub-paragraphs 4.1, 4.3 or 4.6 of this Regulation.

158. The port security assessment shall be performed taking into consideration the requirements referred to in Annex 5 to this Regulation.

159. If during assessment of the port facilities a SPSI inspector has established that the protected territory of this port facility covers the entire port, security requirements applicable to the port facilities shall have a priority over security requirements applicable to the port.

160. A SPSI inspector shall prepare a port security assessment, by including in it the information based on the elements of the port security assessment referred to in Annex 5 to this Regulation, and submit it for approval to the Director of the Maritime Security Department.

161. The port security assessment shall be prepared in two counterparts. One counterpart of the assessment shall be sent to the port authority, while the other shall be stored by the SPSI.

162. A SPSI inspector shall issue the recommendations and instructions to the ports or the territories adjacent to them referred to in Paragraph 157 of this Regulation regarding the security measures to be included in the port security plan by indicating the priority security measures and deadline for submission of the security plan.

163. If any changes to the port or risks thereto have occurred, the port authority has an obligation to immediately provide the relevant information to the SPSI. Based on the this current information regarding changes to the port or risks thereto, the SPSI inspector shall evaluate the port security and, where necessary, make amendments to the port security assessment. Amendments shall be approved by the Director of the Maritime Security Department.

164. A SPSI inspector shall, within five working days, inform the port authority regarding results of the port security assessment.

165. A SPSI inspector shall perform a full port security assessment at least once in five years. The port security assessment may be prepared by a recognised security organisation if it is certified for performance of such task. In such case, the port security assessment prepared by it shall be approved by the Director of the Maritime Security Department.

**4.3. Port Security Authority**

166. Each port has a port security authority responsible for the security matters at the port, including for preparation and implementation of the port security plan.

167. The relevant port authority shall perform the functions of the port security authority within the protected territory of its port.

**4.4. Port Security Officer**

168. The SPSI at a written request of the port security authority shall approve a port security officer for each protected territory of the port.

169. A candidate for the port security officer proposed by the port security authority shall be approved if he or she conforms to the requirements set for the port facility security officer referred to in Part A, Sub-paragraph 18.1 of the ISPS Code.

170. If the SPSI establishes that the approved port security officer does not any longer conform to the requirements laid down in Paragraph 169 of this Regulation, it may take a decision to revoke the approval of the port security officer and request the port security authority to propose another candidate for the position of port security officer.

171. One port security officer may be approved for several ports.

172. The port security officer shall perform the duties related to port security (by analogy with the duties for the port facility security officer referred to in Part A, Paragraphs 17 and 18 of the ISPS Code), and shall be a contact person in the matters related to port security.

173. If the port security officer is not at the same time also a port facility security officer, the port security officer shall cooperate with the port facility security officers at the relevant port and coordinate their actions in security matters.

174. The port security officer may be replaced only by a person conforming to the requirements laid down for the port facility security officer in Part A, Sub-paragraph 18.1 of the ISPS Code. The SPSI shall not separately approve this person, and his or her conformity to the requirements referred to in this Paragraph is verified by the SPSI during the port security verifications.

**4.5. Preparation and Approval of the Port Security Plan and Amendments Thereto**

175. The port security plan or any amendments thereto shall be prepared by the port security officer. The port security plan or amendments thereto may be prepared by a recognised security organisation if it is certified for performance of such task. The port security plan or any amendments thereto shall be prepared in compliance with the following conditions:

175.1. the port security plan shall be prepared in accordance with the structure of the plan referred to in Annex 6 to this Regulation;

175.2. the requirements referred to in Annex 7 to this Regulation shall be applied to drafting of some content elements of the port security plan (when drafting a content of the rest of the port security plan, requirements and recommendations laid down by Annex II, Paragraph 16 to Council Regulation No. 725/2004 for the port facility security plans shall be applied by analogy);

175.3. if the port services ro-ro vessels, the port security plan shall include special security measures applicable to the passengers and vehicles to be transported by ro-ro vessels;

175.4. the port security plan shall include the security plans of the port facilities on its territory;

175.5. the following information shall be used for the preparation of the port security plan and amendments thereto:

175.5.1. the information included in the port security assessment;

175.5.2. conclusions drawn by analysing the information included in the port security assessment;

175.5.3. conclusions drawn by analysing the actual circumstances in the port;

175.5.4. conclusions drawn by analysing the recommendations made by the SPSI or the institutions connected with State security (for example, the State Police, the Security Police, the State Border Guard, the Naval Forces Flotilla of the National Armed Forces, the State Fire-fighting and Rescue Service);

175.5.5. Assessment performed by the Security Police of the information submitted by the SPSI regarding the current risk assessment for the port, if any is requested;

175.6. a port security plan or amendments thereto shall be prepared in Latvian;

175.7. a port security plan may be a part of other plans, and may include other plans besides the plan structure laid down in Annex 6 to this Regulation.

176. The port security plan or amendments thereto together with an application for approval of the port security plan or amendments thereto shall be submitted to the SPSI.

177. A SPSI inspector shall evaluate conformity of the port security plan or amendments thereto to the security requirements, as well as conformity of their appearance to the laws and regulations regarding procedures for developing and drawing up the documents.

178. If during assessment of the port security plan or any amendments thereto a SPSI inspector establishes non-conformities with the requirements referred to in Paragraph 177 of this Regulation, the person preparing the port security plan shall, at the instruction of the SPSI inspector, eliminate the established deficiencies prior to taking a decision to approve the port security plan or amendments thereto.

179. The port security plan or amendments thereto shall be approved in two counterparts, making an appropriate approval note on the front pages of the submitted original port security plan or amendments thereto in accordance with the requirements laid down in the laws and regulations regarding the procedures for developing and drawing up the documents. After approval, one counterpart of the approved plan or amendments thereto shall be sent by the SPSI to the port security authority, while the second original counterpart shall be kept by the SPSI.

180. After approval of the amendments to the port security plan, the port security officer shall ensure that the port security plan is accordingly updated, by changing those pages of the plan where the amendments were made, and making a relevant notation in the amendment recording sheet. The replaced pages with the old wording of the security plan shall be destroyed.

181. In order to ensure compliance of the port security plan with the existing security situation at the port, the port security officer shall review it in full at least once in six months. The training, drills and exercise programme of the port facility security personnel shall be prepared for the next year and submitted to the SPSI by 1 December of the current year. Appropriate information shall be indicated in the section of the port security plan laying down a need for regular revision and updating of the port security plan.

182. The SPSI does not need to approve minor amendments to the port security plan (for example, changes in the contact information of the port and port security officer, changes to the training, drills and exercise plans of the port security personnel, other minor amendments not significantly affecting the port security system).

183. If any changes referred to in Paragraph 182 of this Regulation have taken place, the relevant amendments shall be made in the port security plan, and information on the made amendments shall be provided to the SPSI as soon as possible.

**4.6. Storing of the Port Security Plan, Amendments Thereto and Port Security Records**

184. The parts of the port security plan, draft plan, amendments and draft amendments, as well as the parts of the port security records shall be assigned a status “information for service purposes” and provided with appropriate security in accordance with the Freedom of Information Law and laws and regulations regarding the procedures for protection of information for the service needs.

185. The port security records shall be at least:

185.1. summaries of the port security training, drills and exercises;

185.2. records of the port security incidents and risks;

185.3. records of the infringements in the area of port security;

185.4. records of the change of port security levels;

185.5. records on inspections, maintenance and calibration of the port security equipment;

185.6. records of the implementation of the amendments to the port security plan;

185.7. recording of verifications of the port security system;

185.8. records of the revision of the port security plan;

185.9. records of the revision of the port security assessment;

185.10. security declarations;

185.11. records of the risk to the ship or port facilities, where the ship is located or has been located.

186. One approved counterpart of the port security plan and a counterpart of amendments thereto shall be stored in the port, the second – by the SPSI.

187. Security records of the port shall be stored in the port for at least five years.

**4.7. Port Security Verifications**

188. In order to verify conformity of the port security system with the port security requirements, a SPSI inspector shall perform the security verifications of the port.

189. The SPSI inspector shall perform the following security verifications of the port:

189.1. initial verification – a verification performed prior to initial issuing of the Statement of Security Compliance of the Port to the relevant port;

189.2. annual verification – a verification performed once a year after issuing the Statement of Security Compliance of the Port, in order to regularly verify conformity of the port with the security requirements (period between the verifications shall not be less than 10 months and shall not exceed 12 months);

189.3. renewal verification – a verification performed once in five years prior to reissuance of the Statement of Security Compliance of the Port to the relevant port;

189.4. additional verification – any verification other than the verification referred to Sub-paragraphs 189.1, 189.2 and 189.3 of this Regulation and performed by the inspector to verify constant conformity of the security system to the security requirements, as well as a verification performed based on the information received from other authorities related to State security (for example, the State Police, the Security Police, the State Border Guard, the Naval Force of the National Armed Forces, the State Fire-fighting and Rescue Service) or other legal or natural persons, regarding non-conformity of the port to the security requirements.

190. If deficiencies in the port security system not significantly reducing security of the port are established during any of the verifications referred to in Paragraph 189 of this Regulation, a reverification of the port shall be performed to verify that the deficiencies established during the previous verification are rectified and other deficiencies have not appeared. The port security significantly decreases if the security system is unable to ensure constant complex security of people, ships and other property in the entire object, for example, access control is not provided, designation of restricted access areas and their monitoring or preparation of security declarations is not ensured. If the deficiencies established during any of the verifications referred to in Sub-paragraphs 189.2, 189.3 or 189.4 of this Regulation are not rectified during a reverification, or new deficiencies have occurred, the SPSI shall take a decision to revoke the Statement of Security Compliance of the Port.

191. A SPSI inspector shall perform the port security verification based on the submission of the responsible official of the port security authority, except for the first additional verification.

192. A verification of the port security shall be performed within one day, but if the work load is high (verification may not be performed within one day), time of the verification may be extended to up to two days.

193. Results of the port security verification shall be reflected in the report (annual verification report as the result of the verification referred to in Sub-paragraph 189.2 of this Regulation), providing in it the information regarding the port, type of verification, established deficiencies with a reference to the infringed security requirements. The report shall be signed by the person preparing it and a representative of the port security authority. If the representative of the port security authority refuses to sign the report, an appropriate entry shall be made thereon in the report. The representative of the port security authority or other persons ensuring security of the port shall provide explanations on the deficiencies of the port security system established during verification. The abovementioned explanations shall be attached to the report. A representative of the port security authority has the right to submit comments regarding the content of the report and specify the reasons for his or her refusal to sign it. The comments shall be added to the report.

194. If the results of the initial or renewal verification attest compliance of the port security system to the security requirements, the SPSI inspector shall take a decision to issue the Statement of Security Compliance of the Port.

195. If conformity of the ship to the security requirements is established during any verification referred to in Paragraph 194 of this Regulation, but some deficiencies not significantly reducing port security are discovered, the SPSI inspector shall take a decision to issue the Statement of Security Compliance of the Port and, by taking into account the opinion of the responsible official of the port security authority to the extent possible, lay down a deadline (not later than two months after taking such decision) by which the indicated deficiencies are to be rectified. The port security authority has an obligation to rectify the deficiencies referred to in the decision by the deadline indicated by the inspector.

196. If during any of the verifications referred to in Paragraph 194 of this Regulation it is determined that the port security system does not conform to the security requirements, the SPSI inspector shall take a decision to refuse to issue the Statement of Security Compliance of the Port and lay down a deadline (not later than two months after taking such decision) for the performance of reverification. If a reverification is required, the Statement of Security Compliance of Port shall be issued after performance of the reverification.

197. If the results of the annual verification confirm the conformity of the port security system to the security requirements, the SPSI inspector shall take a decision to make an endorsement in the Statement of Security Compliance of the Port, by indicating in the deadline by which the next verification is to be performed.

198. If conformity of the port to the security requirements is established during the annual verification, but deficiencies not significantly reducing the port security are detected, the SPSI inspector shall, to the extent possible taking into consideration the opinion of the responsible official of the port security authority, indicate a deadline in the deed of annual verification (not later than two months after performance of verification) for elimination of the deficiencies established during the verification, and lay down a deadline for performance of a reverification. If a reverification is required, an endorsement shall be made in the Statement of Security Compliance of the Port only after performance of the reverification. The port security authority has an obligation to rectify the deficiencies referred to in the verification deed by the deadline indicated by the SPSI inspector.

199. If it is determined in the annual verification that the port security system does not conform to the security requirements, the SPSI inspector shall take a decision to revoke the Statement of Security Compliance of the Port.

200. After additional verification of the port, the SPSI inspector shall prepare a report referred to in Paragraph 193 of this Regulation and take one of the following decisions:

200.1 regarding conformity of the port to the security requirements if the port conforms to security requirements;

200.2 regarding conformity of the port to security requirements with a task to rectify the deficiencies established during the verification, which do not significantly reduce port security, and, to the extent possible taking into account the opinion of the responsible official of the port security authority, indicate the deadline (not later than two months after taking such decision) for rectification of these deficiencies, and determine a deadline for a reverification. The port security authority has an obligation to rectify the deficiencies referred to in the decision by the deadline indicated by the SPSI inspector;

200.3 regarding non-conformity of the port to security requirements and revocation of the Statement of Security Compliance of the Port (if any issued), if the port does not conform to the security requirements.

201. A SPSI inspector shall, during the port security verification, verify conformity of the port security system to the port security requirements.

**4.8. Statement of Security Compliance of the Port**

202. Statement of Security Compliance of the Port (Annex 8) shall be issued by the SPSI after performance of the verification referred to in Sub-paragraph 189.1 or 189.3 of this Regulation.

203. A SPSI shall, within five working days after taking the decisions referred to in Paragraph 194 of this Regulation, issue a Statement of Security Compliance of the Port to the port security authority.

204. The Statement of Security Compliance of the Port shall be issued for a period of up to five years. The Statement of Security Compliance of the Port may be issued for a period shorter than five years if:

204.1. the SPSI has in its possession justified information regarding the planned change of the actual circumstances in respect of the port during the period shorter than five years from issuing of Statement of Security Compliance of the Port (for example, reconstruction or termination of the operation of the port, change of the port security system, change of the port owner or possessor is planned);

204.2. a relevant written request is received from the port security authority.

205. If the Statement of Security Compliance of the Port is damaged, lost or stolen, port security authority shall immediately notify the SPSI thereof.

206. A new Statement of Security Compliance of the Port, if the term of validity thereof has expired, shall be issued by the SPSI after the verification referred to in Sub-paragraph 189.3 of this Regulation.

207. The Statement of Security Compliance of the Port shall become invalid if the port security authority has not ensured performance of the verification referred to in Sub-paragraph 189.2 of this Regulation by the deadline indicated by the SPSI.

**5. Declaration of Security**

208. A Declaration of Security shall be completed at the request of the ship security officer or port facility security officer in accordance with Part A, Paragraph 5 of the ISPS Code prior to ship and port interface or ship to ship activity in the following cases:

208.1. if the ship or port facility involved in interface operates on different levels or at the second and third security level;

208.2. if a security incident or security threat has occurred during the last three ship and port interfaces or ship to ship activities;

208.3. if a security incident or security threat has occurred during the last month in the port facility involved in the interface;

208.4. if the ship, which complies with the security requirements, is interfacing with the port facility whereto the security requirements are not applicable;

208.5. if the ship, which complies with the security requirements, has an activity with the ship whereto the security requirements are not applicable;

208.6. if the port facility, which complies with the security requirements, is interfacing with the ship whereto the security requirements are not applicable;

208.7. if the port facility, which complies with the security requirements, is interfacing with the ship whereto the security requirements are applicable but they are not complied with, for example, the ship is operated without a valid International Ship Security Certificate or Interim International Ship Security Certificate (certificate is not valid if intermediate verification approvals have not been made by the laid down deadlines, or if its term of validity has expired, and it is not extended in accordance with the procedures laid down in the ISPS Code);

208.8. in any other case of the ship and port interface or ship to ship activity laid down in the ship or port facility security plan.

209. In the cases referred to in Paragraph 208 of this Regulation a Declaration of Security shall be completed each time of the ship and port interface or ship to ship activity. If the ship interface with the relevant port facility or ship is regular, one declaration of security may be prepared for a period not exceeding three months.

210. Completed Declarations of Security shall be kept on board the ship for at least last 10 visits to the ports.

211. Declaration of Security completed in the port facilities shall be available for at least last five years.

**6. Setting the Security Level**

212. The Security Police shall set the security level of a ship, port, port section or port facility according to Part A, Sub-paragraphs 2.1.9, 2.1.10 and 2.1.11 of the ISPS Code and inform the Coast Guard of the decision taken, which shall make a relevant note in the national SSN system.

213. The Security Police shall take a decision referred to in Paragraph 212 of this Regulation after receipt and assessment of the information from other authorities related to State security (for example, the State Police, the Security Police, the State Border Guard, the Naval Force of the National Armed Forces, the State Fire-fighting and Rescue Service) or other institutions, legal or natural persons of the Republic of Latvia or foreign countries.

214. The Maritime Administration shall provide the Security Police with the information in its possession regarding security of ships, ports and port facilities for the Security Police to be able to set a security level for the ship, port, section of port or a port facility in accordance with Paragraph 212 of this Regulation.

215. The Security Police shall ensure the fulfilment of the requirements of Part A, Sub-paragraphs 4.1 and 4.2, and Part B, Sub-paragraph 4.21 of the ISPS Code.

**7. Approval of the Training Programmes for Personnel**

216. Prior to commencement of security training of the port or port facility personnel (port or port facility security officer, port or port facility personnel with specific responsibilities related to security, other port or port facility personnel), a person planning to perform training shall submit a training programme to the SPSI together with a submission for approval of the training programme.

217. The training programme shall be submitted to the SPSI in two counterparts.

218. A SPSI inspector shall, within one month from receiving the training programme, evaluate conformity of its content with the security requirements and the requirements of Part A, Paragraph 18 of the ISPS Code, and:

218.1. if non-conformities were not established, take a decision to approve the programme, by making an approval note on the first page of the submitted programme in accordance with the laws and regulations regarding developing and drawing up the documents, and issue one counterpart of the approved programme to the submitter;

218.2. if any non-conformities are established, take a decision to refuse to approve the programme and return it to the submitter for rectification of the established non-conformities. After rectification of non-conformities the person planning the training may repeatedly submit the programme to the SPSI for approval.

219. Assessment and implementation of the content of the training course programme for the ship security officers and ship personnel, the duties whereof include performance of the ship security functions, shall be carried out by the Seafarer Register of the Maritime Administration in accordance with the laws and regulations regarding certification and supervision of the professional preparation programmes of seafarers.

**8. Basic Requirements for Ship and Company, Port and Port Facility Security Training, Drills and Exercises**

220. A company, port security authority, owner or possessor of the port facility shall ensure that the ship and company, port or port facility security training takes place at least once a year, but not less frequently than once in 18 months.

221. Communication, coordination, resource availability and response shall be tested during the security exercises, and the authorities and officials referred to in Part B, Paragraph 13.7 or 18.6 of the ISPS Code may participate in it.

222. The security exercises may be:

222.1. a full range or partial range exercises;

222.2. a practical or theoretical simulation or seminar;

222.3. combined with other exercises (for example, exercises for response in emergency situation or exercises on the ship, at the port or in the port facility requested by the competent authority of other country).

223. A company, port security authority, owner or possessor of the port facility shall, within a week after the ship and company, port or port facility security exercises, submit a report thereon to the SPSI.

224. A company, port security authority, owner or possessor of the port facility shall ensure security drills of the ship and port facility in accordance with the requirements of Part B, Sub-paragraph 13.6 or 18.5 of the ISPS Code.

225. Individual elements of the security plan shall be taught and tested during the security drills.

226. Training of the port and port facility security officers shall be carried out as needed, but not less frequently than once in three years. After completion of the training course, the port and port facility security officer shall submit to the SPSI the documents attesting to completion of the course (for example, certificate on completion of the preparation courses, certificate or other confirmation of completion of the training for the port or port facility security officer).

227. The training of the port and port facility personnel having responsibilities related to security and of other port and port facility shall be carried out as needed, but not less frequently than once a year in accordance with the approved security training programmes.

228. The training, drills and exercises of the port and port facility personnel having responsibilities related to security and of other port and port facility personnel shall be planned and implemented by either the port or port facility security officer or a recognised security organisation.

229. Security training of port and port facility officers may be carried out only by a recognised security organisation.

230. The ship and company, port and port facility training, drills and exercise plan for the following year shall be submitted to the SPSI by 30 December of the current year. A report of the course of training shall be submitted to the SPSI within thirty days after completion of the training.

**9. Exchange of Information and Cooperation**

231. The Maritime Administration shall exchange information with the International Maritime Organization, the European Commission and other European Union Member States in accordance with Article 4 of Council Regulation No 725/2004 and Chapter XI-2, Regulation 13 of the SOLAS Convention.

232. The Coast Guard shall ensure fulfilment of the requirements referred to in Part B, Sub-paragraphs 4.13, 4.15, 4.16 (except for provision of information to the International Maritime Organization), 4.22, 4.23 and 4.24 of the ISPS Code. The Coast Guard shall ensure the fulfilment of the requirements, which applies to port facilities, also in respect of ports in general. The Maritime Administration shall provide the information in its possession to the Coast Guard regarding ship, port and port facility security in order for the Coast Guard to be able to provide the information in accordance with this Paragraph. The Coast Guard shall regularly verify the information regarding ship, port and port facility security.

233. The Coast Guard shall maintain the national SSN system containing the updated information regarding the places having the port or port facility security plans, as well as contact information regarding the officials responsible for the port or port facility security. The officials responsible for the port or port facility security shall immediately make changes through the national SSN system if the previously submitted contact information has changed.

234. In respect of the international maritime traffic services, the SPSI in the area of security assessment shall cooperate with the relevant European Union Member States.

235. When an international scheduled service is operated between Latvia and one or more European Union Member States, the SPSI may request these countries to exempt the scheduled service from an obligation to provide security information.

236. The Maritime Administration shall provide the European Commission and relevant European Union Member States with a list of the companies and ships which in accordance with Article 7(1) of Council Regulation No 725/2004 and this Regulation are exempted from an obligation to provide security information.

237. The Maritime Administration shall provide to the European Commission a list of the ports to which this Regulation applies, and inform the European Commission regarding any changes to the abovementioned list.

238. Ship, port and port facility security officers shall cooperate to ensure more comprehensive ship, port and port facility security, and shall be contact persons in the matters related to ship, port or port facility security accordingly.

239. In order to enhance ship, port and port facility security and to ensure the exchange of mutual information, the authorities referred to in this Regulation and, where necessary, other competent authorities may develop operational action plans.

240. The Naval Forces Flotilla of the National Armed Forces shall ensure the boarding of MSI and SPSI inspectors on the ship located in the territorial waters of the Republic of Latvia, for the performance of security control measures, utilising the technical assets, naval platforms or aircraft of the National Armed Forces.

**10. Submission of Documents and Appealing of Decisions**

241. If the documents provided for in this Regulation are submitted as electronic documents prepared in accordance with laws and regulations regarding drafting electronic documents, they shall be submitted in one counterpart.

242. A decision referred to in this Regulation may be contested and appealed in accordance with the procedures laid down in the Maritime Administration and Marine Safety Law.

**11. Closing Provisions**

243. Cabinet Regulation No. 682 of 22 August 2006, Regulations Regarding the Division of Functions of Ship and Shipping Company, Port and Port Facility Security (*Latvijas Vēstnesis*, 2006, No. 138), is repealed.

244. Cabinet Regulation No. 748 of 13 November 2007, Regulations Regarding the Division and Supervision of Functions of Ship and Company, Port and Port Facility Security (*Latvijas Vēstnesis*, 2007, No. 188; 2014, No. 85), is repealed.

245. The port facility and port security plans approved prior to coming into force of this Regulation shall be applicable until making current necessary amendments therein.

**Informative Reference to the European Union Directive**

This Regulation includes the legal norms arising from Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security.

Prime Minister Laimdota Straujuma

Acting for the Minister of Transport, Minister for the Interior Rihards Kozlovskis

**Annex 1**

Cabinet Regulation No. 746

22 December 2015

|  |  |  |  |
| --- | --- | --- | --- |
| Place for the issuer’s symbol |  |  |  |

**STARPTAUTISKAIS KUĢA AIZSARDZĪBAS SERTIFIKĀTS**

***INTERNATIONAL SHIP SECURITY CERTIFICATE***

|  |  |  |
| --- | --- | --- |
| Sertifikāta numurs  *Certificate number* |  | Latvijas Republika/*Republic of Latvia* |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Saskaņā ar Starptautiskā kuģu un ostu iekārtu aizsardzības kodeksa (ISPS kodeksa) noteikumiem Latvijas Republikas valdības vārdā izsniegusi Latvijas Jūras administrācija | | | | | |
| *Issued under the provisions of the International Code for the Security of Ships and of Port Facilities (ISPS Code) under the authority of the Government of Republic of Latvia by Maritime Administration of Latvia* | | | | | |
| Kuģa vārds |  |  | Identifikācijas numurs vai apzīmējums ar burtiem | |  |
| *Name of ship* |  |  | *Distinctive number or letters* | |  |
| Kuģa pieraksta osta |  |  | Kuģa tips |  | |
| *Port of registry* |  |  | *Type of ship* |  | |
| Bruto tilpība |  |  | IMO numurs |  | |
| *Gross tonnage* |  |  | *IMO number* |  | |

|  |  |
| --- | --- |
| Kuģošanas kompānijas nosaukums un adrese |  |
| *Name and address of the maritime company* |  |

|  |  |
| --- | --- |
| Kuģošanas kompānijas identifikācijas numurs |  |
| *Maritime company identification number* |  |

|  |  |
| --- | --- |
| AR ŠO TIEK APLIECINĀTS, KA: | |
| *THIS IS TO CERTIFY THAT:* | |
| 1. | kuģa aizsardzības sistēma un viss ar kuģa aizsardzību saistītais aprīkojums ir pārbaudīts saskaņā ar ISPS Kodeksa A daļas 19.1. punktu prasībām; |
| *the security system and any associated security equipment of the ship has been verified in accordance with Section 19.1 of Part A of the ISPS Code;* |
| 2. | pārbaude pierādīja, ka kuģa aizsardzības sistēma un ar kuģa aizsardzību saistītais aprīkojums visos aspektos ir apmierinošs un kuģis atbilst Konvencijas XI-2 daļas un ISPS Kodeksa A daļas prasībām; |
| *the verification showed that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of Chapter XI-2 of the Convention and Part A of the ISPS Code;* |
| 3. | kuģim ir apstiprināts kuģa aizsardzības plāns. |
| *the ship is provided with an approved ship security plan.* |

|  |  |
| --- | --- |
| Datums, kad veikta sākotnējā/atkārtotā pārbaude, uz kuru pamatojoties šis sertifikāts ir izsniegts |  |
| *Date of initial/renewal verification on which this certificate is issued* |  |

|  |  |  |
| --- | --- | --- |
| Šis sertifikāts derīgs līdz |  |  |
| *This certificate is valid until* |  |  |
| un ir pakļauts pārbaudēm atbilstoši ISPS Kodeksa A daļas 19.1.1 punkta prasībām | | |
| *and is subject to verifications in accordance with Section 19.1.1 of Part A of the ISPS Code* | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Izsniegts | |  |  | |
| *Issued at* | |  |  | |
|  | |  |  | |
| Izsniegšanas datums | |  |  | |
| *Date of issue* | |  | |  |
|  | http://likumi.lv/wwwraksti/2015/254/BILDES/SEAL1.PNG | | | sertifikātu izsniegušās amatpersonas paraksts/  *signature of the duly authorized official issuing the certificate* |

|  |
| --- |
| Starpposma pārbaudes apstiprinājums |
| *Endorsement for intermediate verification* |
| Apliecinu, ka ISPS kodeksa A daļas 19.1.1. punktā paredzētās starpposmu pārbaudes laikā konstatēts, ka kuģis atbilst Konvencijas XI-2 nodaļas un ISPS Kodeksa a daļas attiecīgajiem noteikumiem. |
| *THIS IS TO CERTIFY that at an intermediate verification required by Section 19.1.1 of Part A of the ISPS Code the ship was found to comply with the relevant provisions of Chapter XI-2 of the Convention and Part A of the ISPS Code.* |

|  |  |  |
| --- | --- | --- |
| Starpposma pārbaude | | |
| *Intermediate verification* |  |  |
|  |  |
|  | Paraksts un tā atšifrējums/*signature and deciphering* |

|  |  |  |  |
| --- | --- | --- | --- |
| Vieta |  | |  |
| *Place* |  | |
| Datums |  | |
| *Date* | | |
| Z.v.  *Seal or stamp* | | |
| Papildu pārbaužu apstiprinājums | | | |
| *Endorsement for additional verification* | | | |
| Papildu pārbaude | |  | |
| *Additional verification* | |  | |
|  | |  | |
|  | | Paraksts un tā atšifrējums/*signature and deciphering* | |
|  | |  | |

|  |  |  |
| --- | --- | --- |
| Vieta |  |  |
| *Place* |  |
| Datums |  |
| *Date* | |
| Z.v.  *Seal or stamp* | |

|  |  |
| --- | --- |
| Papildu pārbaude |  |
| *Additional verification* |  |
|  |  |
|  | Paraksts un tā atšifrējums/*signature and deciphering* |

|  |  |  |
| --- | --- | --- |
| Vieta |  |  |
| *Place* |  |
| Datums |  |
| *Date* | |
| Z.v.  *Seal or stamp* | |

|  |  |
| --- | --- |
| Papildu pārbaude |  |
| *Additional verification* |  |
|  |  |
|  | Paraksts un tā atšifrējums/*signature and deciphering* |

|  |  |  |
| --- | --- | --- |
| Vieta |  |  |
| *Place* |  |
| Datums |  |
| *Date* | |
| Z.v.  *Seal or stamp* | |

|  |  |  |
| --- | --- | --- |
| Papildu pārbaude saskaņā ar ISPS Kodeksa A daļas 19.3.7.2. punktu | | |
| *Additional verification in accordance with Section A/19.3.7.2 of the ISPS Code* | | |
|  | | |
| Apliecinu, ka ISPS Kodeksa A daļas 19.3.7.2. punktā noteiktās papildu pārbaudes laikā konstatēts, ka kuģis atbilst Konvencijas XI-2 nodaļas un ISPS kodeksa a daļas attiecīgajiem noteikumiem. | | |
| *THIS IS TO CERTIFY that during an additional verification required by Section 19.3.7.2 of Part A of the ISPS Code the ship was found to comply with the relevant provisions of Chapter XI-2 of the Convention and Part A of the ISPS Code.* | | |
|  | |  |
|  | Paraksts un tā atšifrējums/*signature and deciphering* | |

|  |  |  |
| --- | --- | --- |
| Vieta |  |  |
| *Place* |  |
| Datums |  |
| *Date* | |
| Z.v.  *Seal or stamp* | |

|  |  |
| --- | --- |
| Apstiprinājums, lai pagarinātu apliecību, ja tā ir derīga mazāk par 5 gadiem, gadījumos, kad piemērojams ISPS Kodeksa A daļas 19.3.3. punkts | |
| *Endorsement to extend the certificate if valid for less than 5 years where Section A/19.3.3 of the ISPS Code applies* | |
|  | |
| Kuģis atbilst ISPS Kodeksa A daļas attiecīgajiem noteikumiem, un sertifikāts saskaņā ar ISPS  Kodeksa A daļas 19.3.3. punktu ir derīgs līdz  ....................................................................................... | |
| *The ship complies with the relevant provisions of Part A of the ISPS Code, and the certificate shall, in accordance with Section 19.3.3 of Part A of the ISPS Code, be accepted as valid until*  ....................................................................................... | |
|  |  |
|  | Paraksts un tā atšifrējums/*signature and deciphering* |

|  |  |  |
| --- | --- | --- |
| Vieta |  |  |
| *Place* |  |
| Datums |  |
| *Date* | |
| Z.v.  *Seal or stamp* | |

|  |  |  |  |
| --- | --- | --- | --- |
| Apstiprinājums gadījumos, kad pabeigta atkārtotā pārbaude un ir piemērojams ISPS Kodeksa A daļas 19.3.4. punkts | | | |
| *Endorsement where the renewal verification has been completed and Section A/19.3.4 of the ISPS Code applies* | | | |
|  | | | |
| Kuģis atbilst ISPS Kodeksa A daļas attiecīgajiem noteikumiem, un sertifikāts saskaņā ar ISPS Kodeksa A daļas 19.3.4. punktu ir derīgs līdz .......................................................................................................... | | | |
| *The ship complies with the relevant provisions of Part A of the ISPS Code, and the certificate shall, in accordance with Section 19.3.4 of Part A of the ISPS Code, be accepted as valid until* .......................................................................................................... | | | |
|  | |  | |
|  | | Paraksts un tā atšifrējums/*signature and deciphering* | |
| Vieta |  | |  |
| *Place* |  | |
| Datums |  | |
| *Date* | | |
| Z.v.  *Seal or stamp* | | |

|  |  |  |
| --- | --- | --- |
| Apstiprinājums, lai pagarinātu sertifikāta derīguma termiņu, kamēr tiek sasniegta pārbaudes osta, gadījumos, kad piemērojams ISPS kodeksa A daļas 19.3.5. punkts vai ISPS kodeksa A daļas 19.3.6. punkts | | |
| *Endorsement to extend the validity of the certificate until reaching the port of verification where Section A/19.3.5 of the ISPS Code applies or for a period of grace where Section A/19.3.6 of the ISPS Code applies* | | |
|  | | |
| Šis sertifikāts saskaņā ar ISPS Kodeksa A daļas 19.3.5./19.3.6. punktu ir derīgs līdz  ...................................................................... | | |
| *This certificate shall, in accordance with Section 19.3.5/19.3.6 of Part A of the ISPS Code, be accepted as valid until*  ...................................................................... | | |
|  | http://likumi.lv/wwwraksti/2015/254/BILDES/SEAL1.PNG |  |
|  |  | Paraksts un tā atšifrējums/ |
|  |  | *signature and deciphering* |

|  |  |  |
| --- | --- | --- |
| Vieta |  |  |
| *Place* |  |
| Datums |  |
| *Date* | |
| Z.v.  *Seal or stamp* | |

|  |  |  |
| --- | --- | --- |
| Apstiprinājums, lai pagarinātu sertifikāta derīguma termiņu gadījumos, kad piemērojams ISPS Kodeksa A daļas 19.3.7.1. punkts | | |
| *endorsement for advancement of expiry date where Section A/19.3.7.1 of the ISPS code applies* | | |
|  | | |
| Saskaņā ar ISPS Kodeksa A daļas 19.3.7.1. punktu jaunais derīguma termiņš beidzas  ................................................................................. | | |
| *In accordance with Section 19.3.7.1 of Part A of the ISPS Code, the new expiry date is*  ................................................................................. | | |
|  | http://likumi.lv/wwwraksti/2015/254/BILDES/SEAL1.PNG | Paraksts un tā atšifrējums/ |
|  | *signature and deciphering* |
| Vieta |  |
| *Place* |  |
| Datums |  |
| *Date* |  |

Acting for the Minister of Transport, Minister for the Interior Rihards Kozlovskis

**Annex 2**

Cabinet Regulation No. 746

22 December 2015

|  |  |  |  |
| --- | --- | --- | --- |
| Place for the issuer's symbol |  |  |  |

**STARPTAUTISKAIS KUĢA AIZSARDZĪBAS PAGAIDU SERTIFIKĀTS**

**INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE**

|  |  |  |
| --- | --- | --- |
| Sertifikāta numurs  *Certificate number* |  | Latvijas Republika/*Republic of Latvia* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Saskaņā ar Starptautiskā kuģu un ostu iekārtu aizsardzības kodeksa (ISPS kodeksa) noteikumiem Latvijas Republikas valdības vārdā izsniegusi Latvijas Jūras administrācija | | | | |
| *Issued under the provisions of the International Code for the Security of Ships and of Port Facilities (ISPS Code) under the authority of the Government of Republic of Latvia by Maritime Administration of Latvia* | | | | |
| Kuģa vārds |  |  | Identifikācijas numurs vai apzīmējums ar burtiem |  |
| *Name of ship* |  |  | *Distinctive number or letters* |  |
| Kuģa reģistrācijas osta |  |  | Kuģa tips |  |
| *Port of registry* |  |  | *Type of ship* |  |
| Bruto tilpība |  |  | IMO numurs |  |
| *Gross tonnage* |  |  | *IMO number* |  |

|  |  |
| --- | --- |
| Kuģošanas kompānijas nosaukums un adrese |  |
| *Name and address of the maritime company* |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Kuģošanas kompānijas identifikācijas numurs | | | |  | | |
| *Maritime company identification number* | | | |  | | |
| APLIECINU, ka kuģis atbilst ISPS Kodeksa A daļas 19.4.2. punktā noteiktajām prasībām | | | | | | |
| *THIS IS TO CERTIFY THAT the requirements of Section A/19.4.2. of the ISPS Code have been complied with* | | | | | | |
|  | | | | | | |
| Sertifikāts ir izsniegts saskaņā ar ISPS Kodeksa A. daļas 19.4. punktu | | | | | | |
| *This Certificate is issued in accordance with Section A/19.4 of the ISPS Code* | | | | | | |
| Šis sertifikāts derīgs līdz | |  | | |  | |
| *This certificate is valid until* | |  | | |  | |
| Izsniegšanas vieta |  | | |  | | |
| *Issued at* |  | | |  | | |
|  | http://likumi.lv/wwwraksti/2015/254/BILDES/SEAL1.PNG | | |  | | |
| Izsniegšanas datums |  | | |  | | |
| *Date of issue* |  | | sertifikātu izsniegušās amatpersonas paraksts/  *signature of the duly authorized official issuing the certificate* | | |  |

Acting for the Minister of Transport, Minister for the Interior Rihards Kozlovskis

**Annex 3**

Cabinet Regulation No. 746

22 December 2015

**Structure of the Port Facility Security Plan**

I. Name of the port facility.

II. Reference to other plans incorporating this plan.

III. Developer of the plan.

IV. Date of the plan approval.

V. Position, signature and full name of the official approving the plan.

VI. Contact information of the port facility security officer.

VII. List of amendments to the plan.

VIII. Table of contents of the plan.

1. Introduction:

1.1. purpose;

1.2. situation;

1.3. information important for planning;

1.4. assumptions.

2. Description of the port facility:

2.1. location, boundaries, breakdown by zones;

2.2. adjacent territories, their impact;

2.3. maps, plans.

3. Port facility security organisation:

3.1. port facility security officer;

3.2. by-laws (in annex);

3.3. structure, personnel, its breakdown by work place, changes related to change of security levels;

3.4. work schedules, rotation, rest breaks and conditions laid down for the personnel;

3.5. rights and obligations of the personnel;

3.6. personnel instructions (in annex);

3.7. identification of the port facility security personnel:

3.7.1. uniforms;

3.7.2. identification documents and signs;

3.8. identification of the port facility security transportation;

3.9. port facility security council;

3.10. relation to other security and safety structures;

3.11. control procedures for maintaining of security measures.

4. Port facility security equipment:

4.1. perimeter fences, gates, doors, barriers:

4.1.1. layout;

4.1.2. physical description;

4.1.3. warning signs;

4.1.4. evaluation criteria of the condition;

4.1.5. procedures for verification of the condition and rectification of defects;

4.1.6. action in the case of impairments;

4.2. lighting:

4.2.1. layout;

4.2.2. physical description;

4.2.3. evaluation criteria of the condition of lighting devices;

4.2.4. procedures for verification of the lighting devices and rectification of defects;

4.2.5. action in the case of malfunction of lighting devices;

4.3 other security and safety equipment (for example video surveillance, alarm, access control system):

4.3.1. listing, layout, description;

4.3.2. evaluation criteria of the equipment condition;

4.3.3. procedures for verification of the equipment condition and rectification of defects;

4.3.4. action in the case of malfunction of equipment.

5. Port facility security measures (at security level 1, 2 and 3) 1:

5.1. procedures for control of entrance passes:

5.1.1. distribution of people, transportation and cargo flow among entrance points, working hours;

5.1.2. entry pass control:

5.1.2.1. for employees;

5.1.2.2. for suppliers of cargoes;

5.1.2.3. for suppliers of ship inventory;

5.1.2.4. for passengers;

5.1.2.5. for representatives of State authorities;

5.1.2.6. for members of the ship crew;

5.1.2.7. for visitors;

5.1.3. identification system for people and transportation:

5.1.3.1. types and samples of identification documents and entrance passes;

5.1.3.2. issuing of identification documents and entrance passes;

5.1.3.3. checking of identification documents and entrance passes at the entrance points;

5.1.4. action in the case of infringements of the entrance procedures;

5.2. monitoring of restricted access areas:

5.2.1. restricted access areas, their boundaries, entrance points and description;

5.2.2. designations of the restricted access areas;

5.2.3. security measures, instructions;

5.2.4. procedures for the access control:

5.2.4.1. for passengers;

5.2.4.2. for employees;

5.2.4.3. suppliers of cargoes;

5.2.4.4. for suppliers of ship inventory;

5.2.4.5. for members of the ship crew;

5.2.4.6. for representatives of State authorities;

5.2.4.7. for visitors;

5.2.5. action in the case of infringements of the laid down regime of the restricted access area;

5.3. monitoring of cargo operations:

5.3.1. procedures for receiving, dispatching and processing cargoes;

5.3.2. procedures for drawing up cargo documents;

5.3.3. cargo layout schemes (by types);

5.3.4. cargo security measures and organisation of cargo verifications, instructions;

5.3.5. special measures during processing and recording of dangerous cargoes in the port facility;

5.3.6. action in the case of infringement of the procedures for processing of cargoes;

5.4. monitoring of a ship supply:

5.4.1. procedures for receiving a ship supply;

5.4.2. procedures for drawing up a ship supply documents;

5.4.3. a ship supply security measures and organisation of their verifications, instructions;

5.4.4. action in the case of infringement of the procedures for receiving a ship supply;

5.5. monitoring of the luggage delivered for transportation:

5.5.1. procedures for receiving, dispatching and other processing of luggage;

5.5.2. procedures for drawing up luggage documents;

5.5.3. organisation of luggage security and its verifications, instructions;

5.5.4. action in the event of infringements of the procedures for luggage processing.

6. Announcing security levels:

6.1. powers for announcing and changing security levels;

6.2. procedures for announcing and changing security levels.

7. Drawing up a declaration of security:

7.1. authorisation for the drawing up a declaration of security;

7.2. procedures for the drawing up a declaration of security.

8. Communication:

8.1. in the port facility:

8.1.1. procedures for notification, informing and exchange of information;

8.1.2. communication and notification schemes;

8.2. with the port services and adjacent port facilities:

8.2.1. procedures for notification, informing and exchange of information;

8.2.2. communication and notification schemes;

8.3. with the ship in the port facility:

8.3.1. procedures for notification, informing and exchange of information;

8.3.2. communication and notification schemes;

8.4. with the Maritime Rescue Coordination Centre (MRCC), the Ship and Port Security Inspectorate, water patrols, de-mining and diving units, other security and safety, State and local government authorities:

8.4.1. procedures for notification, informing and exchange of information;

8.4.2. communication and notification schemes.

9. Relation to other security and response plans.

10. Revision of the plan:

10.1. procedures for revision of the plan and making corrections;

10.2. schedule for revision of the plan.

11. Security documentation (records):

11.1. procedures for completing documents;

11.2. sample forms of documents (in annex).

12. Plan security and control:

12.1. allocation and distribution of the plan;

12.2. restrictions and other security measures for the protection of the plan.

13. Training of port facility personnel:

13.1. requirements for professional qualification in relation to port facility security:

13.1.1. port facility security officer;

13.1.2. personnel related to port facility security;

13.1.3. other port facility personnel;

13.2. individual training plans and schedules:

13.2.1. port facility security officer;

13.2.2. personnel related to port facility security;

13.2.3. other port facility personnel;

13.3. plans and schedules for drills;

13.4. plans and schedules for exercises.

14. Plans for emergency situations:

14.1. fire;

14.2. explosion;

14.3. finding a flammable object;

14.4. receiving information regarding bombing threats on a ship;

14.5. information regarding receipt of the signal of the ship security alarm system from a ship in the port facility or its vicinity;

14.6. receipt of information regarding bombing threats at the port or in the port facility:

14.7. a bombing device placed in a letter;

14.8. a bombing device placed in a car;

14.9. a bombing device placed in a boat;

14.10. illegal use of weapons at a port or in a port facility or against it;

14.11. radioactive, chemical or biological contamination;

14.12. leakage of chemical substances;

14.13. leakage of oil and petroleum products;

14.14. demonstrations, pickets;

14.15. strikes;

14.16. crimes, for example, thefts, burglaries;

14.17. unauthorised entry or attempt thereof;

14.18. failure of power supply;

14.19. malfunction of communications;

14.20. discovering of refuges, illegal immigrants and persons without a ticket;

14.21. natural disasters, for example, storms, flood;

14.22. taking of hostages;

14.23. catastrophes with a large number of victims.

15. Deadline for the implementation of security measures.

16. Annexes.

IX. Definitions.

X. List of references and bibliography.

Note.

1 Security measures shall be described by preparing a table. A note regarding implementation of the specific security measure shall be made in the column of the relevant security level.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No. | Measures | Involved forces, means | Level 1 | Level 2 | Level 3 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Acting for the Minister of Transport, Minister for the Interior Rihards Kozlovskis

**Annex 4**

Cabinet Regulation No. 746

22 December 2015

|  |  |  |  |
| --- | --- | --- | --- |
| Place for the issuer's symbol |  |  |  |

**Ostas iekārtas aizsardzības atbilstības apstiprinājums**

*Statement of Security Compliance of the Port Facility*

|  |  |  |
| --- | --- | --- |
| Apstiprinājuma numurs  *Statement No* |  | Latvijas Republika  *Republic of Latvia* |

Izdots saskaņā ar Starptautiskā kuģu un ostu aizsardzības kodeksa (ISPS kodeksa) B daļu

*Issued under the provisions of Part B of the International Code for the Security of Ships and of Port Facilities (ISPS CODE)*

Latvijas Jūras administrācija Latvijas Republikas valdības vārdā

*On behalf of the Government of the Republic of Latvia, the Maritime Administration of Latvia*

|  |  |
| --- | --- |
| Ostas iekārtas nosaukums/*Name of the port facility* |  |
| Ostas iekārtas adrese/*Address of the port facility* |  |

APLIECINU, ka ostas iekārtas atbilstība XI-2 nodaļas un Starptautiskā kuģu un ostu iekārtu aizsardzības kodeksa (ISPS kodeksa) A daļas noteikumiem ir pārbaudīta un ostas iekārta darbojas saskaņā ar apstiprināto ostas iekārtas aizsardzības plānu. Šajā plānā ir apstiprināts:

*THIS IS TO CERTIFY that the compliance of this port facility with the provisions of Chapter XI-2 and Part A of the International Code for the Security of Ships and of Port Facilities (ISPS Code) has been verified and that this port facility operates in accordance with the approved Port Facility Security Plan. This Plan has been approved for the following (specify the types of operations, types of ship or activities or other relevant information):*

|  |
| --- |
|  |
|  |
|  |
|  |
| (norādīt darbības veidus, kuģa tipus, pasākumu veidu vai citu informāciju) |

|  |  |
| --- | --- |
| Atbilstības apstiprinājums ir derīgs līdz |  |
| veicot ikgadējās pārbaudes (kā norādīts nākamajā lappusē) |  |
| *This Statement of Compliance is valid until* |  |
| *subject to annual verifications (as indicated overleaf)* |  |

|  |  |  |
| --- | --- | --- |
| Izsniegšanas vieta/*Place of issue* |  |  |
|  |  |  |
| Izsniegšanas datums/*Date of issue* |  |  |

|  |  |
| --- | --- |
| Pilnvarotā amatpersona, |  |
| kas ir izsniegusi atbilstības apstiprinājumu |  |
| *The duly authorized official issuing the Document* | (paraksts un tā atšifrējums/*signature and deciphering*) |

Z.v.

*Seal*

**Pārbaudes apstiprinājums**

*Endorsement for Verifications*

APLIECINU, ka saskaņā ar ISPS kodeksa B daļas 16.62.4. punktu veiktās pārbaudes laikā konstatēts, ka ostas iekārta atbilst SOLAS Konvencijas XI-2 nodaļas un ISPS kodeksa A daļas attiecīgajiem noteikumiem.

*THIS IS TO CERTIFY that, during a verification carried out in accordance with Paragraph B 16.62.4 of the ISPS Code, the port facility was found to comply with the relevant provisions of Chapter XI-2 of the SOLAS Convention and Part A of the ISPS Code.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. PĀRBAUDE |  | | |  |  |
| Verification |  | | |  |  |
| Vieta |  | | |  |  |
| *Place* |  | | |  |  |
| Datums |  | | |  |  |
| *Date* |  | | |  |  |
| Amatpersona, kas veikusi pārbaudi | | |  |  |  |
|  | | | *(paraksts un tā atšifrējums/signature and deciphering)* | | |
| *Z.v.*  *Seal* | |  | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2. PĀRBAUDE |  | | |  |  |
| Verification |  | | |  |  |
| Vieta |  | | |  |  |
| *Place* |  | | |  |  |
| Datums |  | | |  |  |
| *Date* |  | | |  |  |
| Amatpersona, kas veikusi pārbaudi | | |  |  |  |
|  | | | *(paraksts un tā atšifrējums/signature and deciphering)* | | |
| *Z.v.*  *Seal* | |  | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 3. PĀRBAUDE |  | | |  |  |
| Verification |  | | |  |  |
| Vieta |  | | |  |  |
| *Place* |  | | |  |  |
| Datums |  | | |  |  |
| *Date* |  | | |  |  |
| Amatpersona, kas veikusi pārbaudi | | |  |  |  |
|  | | | *(paraksts un tā atšifrējums/signature and deciphering)* | | |
| *Z.v.*  *Seal* | |  | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 4. PĀRBAUDE |  | | |  |  |
| Verification |  | | |  |  |
| Vieta |  | | |  |  |
| *Place* |  | | |  |  |
| Datums |  | | |  |  |
| *Date* |  | | |  |  |
| Amatpersona, kas veikusi pārbaudi | | |  |  |  |
|  | | | *(paraksts un tā atšifrējums/signature and deciphering)* | | |
| *Z.v.*  *Seal* | |  | | | |

Acting for the Minister of Transport, Minister for the Interior Rihards Kozlovskis

**Annex 5**

Cabinet Regulation No. 746

22 December 2015

**Elements of the Port Security Assessment**

1. In the port security assessment:

1.1. most significant port values and infrastructure necessary to be protected shall be identified and assessed;

1.2. potential threats to the port values and infrastructure and a possibility of these threats shall be identified to determine appropriate security measures and their priority sequence;

1.3. an efficiency level of possible countermeasures and organisational changes shall be assessed in order to reduce deficiencies lowering the port security, and appropriate countermeasures and organisational changes to be performed at the port shall be laid down, as well as their priority sequence;

1.4. deficiencies of infrastructure, administration and procedures performed at the port, including the human factor endangering security of the port shall be identified.

2. In order to comply with the general requirements referred to in Paragraph 1 of this Annex, the port security assessment shall include:

2.1. identification of all territories significant for ensuring security of the port, also by establishing the boundaries of the territory where security requirements shall be applied (protected territory). In the protected territory:

2.1.1. any port territory significant for ensuring of port security may be included;

2.1.2. the port facilities at the port and any adjacent territories subjected to security requirements in accordance with Cabinet Regulation No. 746 of 22 December 2015 Regulations Regarding the Division of Functions, Implementation and Supervision of Ship, Company, Port and Port Facility Security shall be included (port facility assessments made in accordance with Sub-chapter 3.2 shall be used as a basis for assessment of these territories, if such assessments are made for the relevant territories);

2.1.3. the territories adjacent to the port may be included in accordance with Cabinet Regulation No. 746 of 22 December 2015 Regulations Regarding the Division of Functions, Implementation and Supervision of Ship, Company, Port and Port Facility Security;

2.2. the matters significant for port security related to the interaction of the security measures of the port facilities at the port and other port security measures shall be identified;

2.3. the port employees working in the high risk areas and requiring the following shall be identified:

2.3.1. qualification checks;

2.3.2. in-depth checks of security knowledge;

2.4. where necessary, the protected territories shall be divided into areas depending on the risk level of security incidents (areas shall be assessed, taking into consideration not only their possibility of becoming a direct target of threats but also endangerment of this area if the adjacent areas become a target of threats);

2.5. variations of the potential risk of danger in the protected territory shall be identified (for example, seasonal risk);

2.6. specific characteristics of each area in the protected territory significant for port security shall be identified (for example, location, places of access, power supply, communication system, property right, users);

2.7. potential threat scenarios for the port shall be identified, taking into consideration that direct target of specific threats may be the entire port or specific parts of its infrastructure, cargo, luggage, people or transport equipment within the port;

2.8. specific consequences of each potential port threat scenario shall be identified:

2.8.1. taking into consideration that the consequences may be either direct or indirect;

2.8.2. taking into consideration that the consequences could affect both one and several areas of the protected territory;

2.8.3. paying special attention to the risk of human victims;

2.9. possibility of security incident chain effect shall be identified;

2.10. deficiencies in each area of the protected territory reducing its security shall be identified;

2.11. all organisational aspects significant for the general security of the port, including all authorities, rules and procedures related to security shall be identified;

2.12. port security vulnerability in relation to organisational, legislative and procedural aspects shall be identified;

2.13. security measures to reduce the deficiencies lowering the port security shall be identified:

2.13.1. taking into consideration the established differences of the security incident risk levels in different areas of the protected territory;

2.13.2. paying special attention to measures necessary to ensure access control or prohibition of access to the entire port or specific parts of a port, including:

2.13.2.1. for the identification of the passengers, port employees and other workers, visitors of the port and ship crew members;

2.13.2.2. for area or activity monitoring;

2.13.2.3. for cargo and luggage control;

2.14. it shall be identified how measures will be reinforced in the event of an increase of security level;

2.15. it shall be identified how to deal with the situations when an object creating suspicions of danger (for example cargo, luggage, bunker, provisions or persons creating suspicions of danger, unknown parcels, known dangers) is discovered, and the analysis of the conditions is performed in the light of which:

2.15.1. risk shall be cleared where the relevant object is encountered;

2.15.2. risk shall be cleared after moving the relevant object to a secure area;

2.16. security measures shall be identified to limit and mitigate consequences caused by the security incident;

2.17. allocation of security tasks allowing implementation of the necessary security measures based on specific situation and in accordance with the security requirements shall be identified;

2.18. where appropriate, specific attention shall be paid to the relationship with other security plans (for example, port facility security plans) and other already existing security measures, as well as relationship with other response plans (for example, oil spill response plan, port contingency plan, medical intervention plan, nuclear disaster plan);

2.19. necessary requirements shall be laid down for communication to implement security measures;

2.20. measures protecting the information significant for security against unauthorised disclosure shall be laid down;

2.21. level of information necessary for the persons directly involved in ensuring of port security system and other persons shall be identified.

Acting for the Minister of Transport, Minister for the Interior Rihards Kozlovskis

**Annex 6**

Cabinet Regulation No. 746

22 December 2015

**Structure of the Port Security Plan**

I. Name of the port.

II. Reference to other plans incorporating this plan.

III. Reference to other plans being a part of this plan.

IV. Developer of the plan.

V. Date of the plan approval.

VI. Position, signature and full name of the official approving the plan.

VII. Contact information of the port security officer.

VIII. List of amendments to the plan.

IX. Table of contents of the plan.

1. Introduction:

1.1. purpose;

1.2. situation;

1.3. information important for planning;

1.4. assumptions.

2. Description of the port:

2.1. locations, boundaries;

2.2. adjacent territories, their impact;

2.3. territory where security measures shall be implemented:

2.3.1. port facilities where the security measures referred to in the ISPS Code shall be implemented;

2.3.2. adjacent territories;

2.3.3. sub-areas where different security measures shall be implemented;

2.4. maps, plans.

3. Port security organisation1:

3.1. by-laws (in annex);

3.2. structure, employees its breakdown by work place, changes related to change of security levels;

3.3. work schedules, rotation, rest breaks and conditions established for the employees;

3.4. rights and obligations of the employees;

3.5. instructions for employees (in annex);

3.6. identification of the security employees of the port facility:

3.6.1. uniforms;

3.6.2. identification documents and signs;

3.7. identification of the port security transportation;

3.8. port security council;

3.9. relation with other security and safety structures;

3.10. control procedures for maintaining security measures;

3.11. reference to other security plans on the port territory where the security measures shall be implemented.

4. Port security equipment2:

4.1. perimeter fences, gates, doors, barriers:

4.1.1. layout;

4.1.2. physical description;

4.1.3. warning signs;

4.1.4. evaluation criteria of the condition;

4.1.5. procedures for verification of the condition and rectification of defects;

4.1.6. action in the case of impairments;

4.2. lighting:

4.2.1. layout;

4.2.2. physical description;

4.2.3. evaluation criteria of the condition of lighting devices;

4.2.4. procedures for verification of the lighting devices and rectification of defects;

4.2.5. action in the case of malfunction of lighting devices;

4.3. other security and safety equipment (for example video surveillance, alarm, access control systems):

4.3.1. listing, layout, description;

4.3.2. evaluation criteria of the equipment condition;

4.3.3. procedures for verification of the equipment condition and rectification of defects;

4.3.4. action in the case of malfunction of equipment;

4.4. reference to other security plans on the port territory where the security measures shall be implemented.

5. Port security measures (at the security level 1, 2 and 3) 3, 4:

5.1. procedures for control of entrance passes:

5.1.1. distribution of people, transportation and cargo flow among entrance points, working hours;

5.1.2. procedures for control of entrance passes:

5.1.2.1. for employees;

5.1.2.2. for suppliers of cargoes;

5.1.2.3. for suppliers of ship inventory;

5.1.2.4. for passengers;

5.1.2.5. for representatives of State authorities;

5.1.2.6. for members of ship crews;

5.1.2.7. for visitors;

5.1.3. identification system for people and transportation:

5.1.3.1. types and samples of identification documents and entrance passes;

5.1.3.2. issuing of identification documents and entrance passes;

5.1.3.3. checking of identification documents and entrance passes at the entrance points;

5.1.4. action in the case of infringements of the laid down entrance procedures;

5.2. monitoring of restricted access areas:

5.2.1. restricted access areas, their boundaries, entrance points and description;

5.2.2. designations of the restricted access areas;

5.2.3. security measures, instructions;

5.2.4 procedures for access and verification:

5.2.4.1. for passengers;

5.2.4.2. for employees;

5.2.4.3. suppliers of cargoes;

5.2.4.4. for suppliers of ship inventory;

5.2.4.5. for members of ship crews;

5.2.4.6. for representatives of State authorities;

5.2.4.7. for visitors;

5.2.5. action in the case of infringements of the laid down regime of the restricted access area;

5.3. monitoring of cargo operations:

5.3.1. procedures for receiving, dispatching and processing cargoes;

5.3.2. procedures for drawing up cargo documents;

5.3.3. cargo layout schemes (by types);

5.3.4. cargo security measures and organisation of cargo verifications, instructions;

5.3.5. special measures during processing and recording of dangerous cargoes in the port facility;

5.3.6. action in the case of infringement of the laid down procedures for processing cargoes;

5.4. monitoring the supplying of the ship’s stores:

5.4.1. procedures for receiving the ship’s stores;

5.4.2. procedures for drawing up the ship’s stores documents;

5.4.3. security measures for the ship’s stores and organisation of verifications of the ship’s stores, instructions;

5.4.4. action in the case of infringement of the laid down procedures for receiving the ship’s stores;

5.5. monitoring of the luggage delivered for transportation:

5.5.1. procedures for receiving, dispatching and other processing of luggage;

5.5.2. procedures for drawing up luggage documents;

5.5.3. organisation of luggage security and luggage verifications, instructions;

5.5.4. action in the case of infringements of the procedures for luggage processing;

5.6. reference to other security plans on the port territory where the security measures shall be implemented.

6. Announcing security levels:

6.1. powers for announcing and changing security levels;

6.2. procedures for announcing and changing security levels.

7. Drawing up a declaration of security:

7.1. authorisation for the drawing up a declaration of security;

7.2. procedures for the drawing up a declaration of security.

8. Communication:

8.1. with port equipment, adjacent territories and sub-areas where different security measures shall be implemented:

8.1.1. procedures for notification, informing and exchange of information;

8.1.2. communication and notification schemes;

8.2. with port services:

8.2.1. procedures for notification, informing and exchange of information;

8.2.2. communication and notification schemes;

8.3. with ships at the port:

8.3.1. procedures for notification, informing and exchange of information;

8.3.2. communication and notification schemes;

8.4. with the Maritime Rescue Coordination Centre (MRCC), the Ship and Port Security Inspectorate, water patrols, de-mining and diving units, other security and safety, State and local government authorities:

8.4.1. procedures for notification, informing and exchange of information;

8.4.2. communication and notification schemes.

9. Relation to other security and response plans.

10. Revision of the plan:

10.1. procedures for revision of the plan and making corrections;

10.2. schedule for revision of the plan.

11. Security documentation (records):

11.1. procedures for completing documents;

11.2. sample forms of documents (in annex).

12. Plan security and control:

12.1. allocation and distribution of the plan;

12.2. restrictions and other security measures for the protection of the plan.

13. Training of port personnel:

13.1. requirements of professional qualification in relation to port security:

13.1.1. port security officer;

13.1.2. port facility security officers;

13.1.3. personnel related to port facility security;

13.1.4. other port facility personnel;

13.2. individual training plans and schedules:

13.2.1. port security officer;

13.2.2. port facility security officers;

13.2.3. personnel related to port facility security;

13.2.4. other port facility personnel;

13.3. plans and schedules for drills;

13.4. plans and schedules for exercises.

14. Plans for emergency situations:

14.1. fire;

14.2. explosion;

14.3. finding a flammable object;

14.4. receiving information regarding bombing threats on a ship;

14.5. information regarding receipt of the signal of the ship security alarm system from a ship at the port or its vicinity;

14.6. receipt of information on bombing threats at the port or in the port facility:

14.7. a bombing device placed in a letter;

14.8. a bombing device placed in a car;

14.9. a bombing device placed in a boat;

14.10. illegal use of weapons at the port or against it;

14.11. radioactive, chemical or biological contamination;

14.12. leakage of chemical substances and mixtures;

14.13. leakage of oil and petroleum products;

14.14. demonstrations, pickets;

14.15. strikes;

14.16. crimes (for example, thefts, burglaries);

14.17. unauthorised entry or attempt thereof;

14.18. failure of power supply;

14.19. malfunction of communications;

14.20. discovering of refuges, illegal immigrants and persons without a ticket;

14.21. natural disasters (for example, storms, flood);

14.22. taking of hostages;

14.23. catastrophes with a large number of victims.

15. Deadline for the implementation of security measures.

16. Annexes.

X. Definitions.

XI. List of references and bibliography.

Notes.

1General port security organisation concerning all territories at the port whereto security requirements are applied, as well as security organisation of the territories in direct supervision of the port shall be described. In the security organisation of the territories to be included in the port security plan, but where the security measures are to be implemented also in accordance with other security plans, a reference shall be made to already approved security plans of these territories.

2The areas and objects in direct supervision of the port shall be described. In respect of the territories to be included in the port security plan, but in which the security measures are to be implemented also in accordance with other security plans, a reference shall be made to already approved security plans of these territories, except for Sub-paragraph 4.1 of the plan which is to be attributed to the entire territory where the security measures are to be implemented.

3Security measures shall be described by drafting a table. A note regarding implementation of the specific security measure shall be made in the column of the relevant security level.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No. | Measures | Involved forces, means | Level 1 | Level 2 | Level 3 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

4The security measures in the areas and objects in direct supervision of the port shall be described. In respect of the territories to be included in the port security plan, but in which the security measures are to be implemented also in accordance with other security plans, a reference shall be made to already approved security plans of these territories, except for Sub-paragraph 5.1 of the plan which is to be attributed to the entire territory where the security measures are to be implemented.

Acting for the Minister of Transport, Minister for the Interior Rihards Kozlovskis

**Annex 7**

Cabinet Regulation No. 746

22 December 2015

**Content of the Port Security Plan**

**I. General requirements for the content of the port security plan**

1. Port security plan shall:

1.1. define all areas relevant to port security:

1.1.1. taking into consideration that depending on the degree of the risk of danger, security measures may differ in various areas of the port;

1.1.2. paying special attention to the interfaces between port areas with different degree of the risk of danger;

1.2. ensure coordination between security measures for port areas with different degree of the risk of danger;

1.3. where necessary, provide application of different security measures at the port depending on:

1.3.1. different degrees of the risk of danger in different areas of the port;

1.3.2. changes to security level in the entire port or in a particular area of the port;

1.3.3. received specific information (for example, information regarding the object at the port causing suspicions of threat);

1.4. an organisational system shall be laid down ensuring more effective implementation of the security measures.

2. The general requirements referred to in Paragraph 1 of this Annex shall be taken into consideration during the development process of the port security plan, laying down the content elements of the security plan included in Chapter II of this Annex.

**II. Requirements for Individual Content Elements of the Port Security Plan**

3. Requirements for access control:

3.1. if it does not pose any threats to port security, it is permitted to implement access control measures in individual port areas only if the danger level in these areas exceeds an established minimum threshold;

3.2. the access control measures and minimum thresholds of the danger level referred to in Sub-paragraph 3.1 of this Annex shall be laid down in the port security plan;

3.3.by laying down the access control measures, all relevant laws and regulations and positive practice shall be taken into consideration.

4. Requirements for the control of persons, luggage and cargo:

4.1. depending of the degree of the risk of threat, control of the identification documents, luggage and cargo in certain areas of the port need not be applied or applied partially. Persons wishing to enter or located in this areas of the port may be subjected to control;

4.2.if identification cards are used in the port for security reasons, the procedures for their issuing, use control, and return shall be clearly laid down in the port security plan. By developing these procedures, specifics of the certain groups of port users shall be taken into consideration to limit the negative impact of the access control measures on their operation. The aforementioned requirements shall be applicable to the following groups of port users:

4.2.1. seafarers;

4.2.2. officials of State authorities;

4.2.3. persons regularly working at the port or visiting it;

4.2.4. persons whose declared place of residence is located in the port territory;

4.2.5. persons working at the port or visiting it from time to time;

4.3. by laying down the control measures of persons, luggage and cargoes, all relevant laws and regulations and best practice shall be taken into consideration.

5. Where necessary, the procedures for combining of information and formality systems (including pre-arrival formality system) among the persons performing the cargo, luggage and passenger control shall be established in the plan.

6. The measures (including determination of security areas) for the actions with cargoes, luggage, cargo containers, ship’s stores or persons causing suspicions regarding threat to the port, as well as measures in the case of determination of other security problems or infringements shall be laid down in the port security plan.

7. Technical solutions for surveillance of the different port areas and any operations therein shall be laid down in the port security plan.

8. The territories where the access control or any other control is exercised shall be properly signposted.

9. The following communication and security formalities shall be laid down in order to protect security information against unauthorised disclosure:

9.1. exchange of security information takes place in accordance with the security formality standards included in the port security plan;

9.2. depending on the significance of the information, a principle may be observed in respect of exchange of security information that the information is provided only if the requester of information may sufficiently justify a need for the relevant information. The procedures for provision of information to public shall also be included in the port security plan if it does not cause threats to the port security.

10. In order to ensure prompt response, clear procedures regarding a method of notifying the port security officer and port security authority regarding each security incident shall be laid down in the port security plan.

11. Interaction with other plans or actions:

11.1. procedures for interaction of this plan with other security plans in force at the port and security or control actions shall be laid down in the port security plan, where necessary, laying down the procedures for resolution of disputes and rectification of deficiencies;

11.1. procedures for interaction of this plan with other response and emergency plans and corresponding actions, where necessary, laying down the procedures for resolution of disputes and rectification of deficiencies.

12. Procedures for training, drills and exercises shall be laid down in the port security plan.

13. Port security authorities and procedures of their operation:

13.1. port security authorities, allocation of functions among them, as well as procedures of their operation, including the procedures governing cooperation with the port facility officers and ship security officers, where necessary, shall be laid down in detail in the port security plan;

13.2. functions of the port security committee (if any) shall be laid down in the port security plan.

14. Procedures for regular revision and updating of this plan shall be laid down in the port security plan.

Acting for the Minister of Transport, Minister for the Interior Rihards Kozlovskis

**Annex 8**

Cabinet Regulation No. 746

22 December 2015

|  |  |  |  |
| --- | --- | --- | --- |
| Place for the issuer's symbol |  |  |  |

**Ostas aizsardzības atbilstības apstiprinājums**

Statement of Security Compliance of Port

|  |  |  |
| --- | --- | --- |
| Apstiprinājuma numurs  Statement number |  | Latvijas Republika  Republic of Latvia |

Izdots saskaņā ar Latvijas Republikas Ministru kabineta 2015. gada 22. decembra noteikumiem Nr. 746 "Noteikumi par kuģu, kuģošanas kompāniju, ostu un ostas iekārtu aizsardzības funkciju sadalījumu, izpildi un uzraudzību", kas ievieš Eiropas Parlamenta un Padomes 2005. gada 26. oktobra Direktīvu 2005/65/EK par ostu aizsardzības pastiprināšanu

*Issued under the provisions of Regulation No. 746 "Regulations on Subdivision, Implementation and Supervision of Defence Functions of Ships, Maritime Companies, Ports and Port Facilities" of the Cabinet of Ministers of the Republic of Latvia of 22 December 2015, which enforce Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security.*

Latvijas Jūras administrācija Latvijas Republikas valdības vārdā

*On behalf of the Government of the Republic of Latvia, the Maritime Administration of Latvia*

|  |  |
| --- | --- |
| Ostas nosaukums/*Name of the port* |  |
| Ostas adrese/*Address of the port* |  |

APLIECINU, ka ostas atbilstība Latvijas Republikas Ministru kabineta 2015. gada 22. decembra noteikumiem Nr. 746 "Noteikumi par kuģu, kuģošanas kompāniju, ostu un ostas iekārtu aizsardzības funkciju sadalījumu, izpildi un uzraudzību" ir pārbaudīta un osta darbojas saskaņā ar apstiprināto ostas aizsardzības plānu. Šajā plānā ir apstiprināts:

*THIS IS TO CERTIFY that the compliance of this port with the provisions of Regulation No. 746 "Regulations on Subdivision, Implementation and Supervision of Defence Functions of Ships, Maritime Companies, Ports and Port Facilities" of the Cabinet of Ministers of the Republic of Latvia of 22 December 2015 has been verified and that this port operates in accordance with the approved port security plan. This plan has been approved for the following operations with: (specify the types of operations, types of ship or activities or other relevant information)*

|  |
| --- |
|  |
|  |
| (norādīt darbības veidus, kuģa tipus vai pasākumu veidu, vai citu informāciju) |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Atbilstības apstiprinājums ir derīgs līdz | | , | | | | | |  |
| veicot ikgadējas pārbaudes (kā norādīts nākamajā lappusē) | | | | | | | | |
| *This Statement of Compliance is valid until* | | | |  | | |  | |
| *subject to annual verification (as indicated overleaf)* | | | | |  | | | |
| Izsniegšanas vieta/*Place of issue of the statement* | | | | | |  | | |
| Izsniegšanas datums/*Date of issue* |  | | | | | | | |
| Pilnvarotā amatpersona,  kas izsniegusi atbilstības apstiprinājumu | | |  | | | | | |
| *Signature of the authorized official issuing the Statement* | | | (paraksts un tā atšifrējums/*signature and deciphering*) | | | | | |
| Z.v.  *Seal or stamp* | | |  | | | | | |

**Pārbaudes apstiprinājums**

*Endorsement for Verifications*

APLIECINU, ka saskaņā ar Latvijas Republikas Ministru kabineta 2015. gada 22. decembra noteikumiem Nr. 746 "Noteikumi par kuģu, kuģošanas kompāniju, ostu un ostas iekārtu aizsardzības funkciju sadalījumu, izpildi un uzraudzību" veiktās pārbaudes laikā konstatēts, ka osta atbilst attiecīgām šo noteikumu prasībām.

*THIS IS TO CERTIFY that during a verification carried out in accordance with Regulation No. 746 "Regulations on Subdivision, Implementation and Supervision of Defence Functions of Ships, Maritime Companies, Ports and Port Facilities" of the Cabinet of Ministers of the Republic of Latvia of 22 December 2015the port was found to comply with the relevant provisions of these Regulations.*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. PĀRBAUDE | | | |  | | |
| *VERIFICATION* | | | |  | | |
| Vieta |  | | | |  | |
| *Place* |  | | | |  | |
| Datums |  | | | |  |  |
| *Date* |  | | | |  |  |
| Amatpersona, kas veikusi pārbaudi | | |  | | |  |
|  | | | (paraksts un tā atšifrējums/*signature and deciphering of authorized official*) | | | |
| Z.v.  *Seal or stamp* | |  | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2. PĀRBAUDE | | | |  | | |
| *VERIFICATION* | | | |  | | |
| Vieta |  | | | |  | |
| *Place* |  | | | |  | |
| Datums |  | | | |  |  |
| *Date* |  | | | |  |  |
| Amatpersona, kas veikusi pārbaudi | | |  | | |  |
|  | | | (paraksts un tā atšifrējums/*signature and deciphering of authorized official*) | | | |
| Z.v.  *Seal or stamp* | |  | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3. PĀRBAUDE | | | |  | | |
| *VERIFICATION* | | | |  | | |
| Vieta |  | | | |  | |
| *Place* |  | | | |  | |
| Datums |  | | | |  |  |
| *Date* |  | | | |  |  |
| Amatpersona, kas veikusi pārbaudi | | |  | | |  |
|  | | | (paraksts un tā atšifrējums/*signature and deciphering of authorized official*) | | | |
| Z.v.  *Seal or stamp* | |  | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 4. PĀRBAUDE | | | |  | | |
| *VERIFICATION* | | | |  | | |
| Vieta |  | | | |  | |
| *Place* |  | | | |  | |
| Datums |  | | | |  |  |
| *Date* |  | | | |  |  |
| Amatpersona, kas veikusi pārbaudi | | |  | | |  |
|  | | | (paraksts un tā atšifrējums/*signature and deciphering of authorized official*) | | | |
| Z.v.  *Seal or stamp* | |  | | | | |

Acting for the Minister of Transport, Minister for the Interior Rihards Kozlovskis