

## **Guidelines for the development and approval of the ship security plan**

Each ship to which apply the International Code for the Security of Ships and of Port Facilities (ISPS Code), the Convention for the Safety of Life at Sea as amended (SOLAS 74/88) and Regulation (EC) No 725/2004 of the European Parliament and of the Council shall have a ship security plan in an approved electronic format or paper copy, which is developed on the basis of ship security assessment and which provides three security levels.

- (1) To enhance maritime security on board ships the company may designate English language as a working language in ISPS matters and state it in ship security plan.
- (2) The company shall be responsible for preparation and submission for approval of the ship security plan. The ship security plan shall be written in the designated working language in ISPS matters, or the working language of the ship. If the working language used is not English, the translation of the ship security plan into English shall be added on the ships flying the flag of Estonia. If the working language in ISPS matters is other than English the ISPS Code Part A 9.4 and 10.2 requirements still apply and ship security plan and security related records shall be translated into English.
- (3) The Estonian Transport Administration, or a recognized security organization on behalf of the Estonia, shall approve the ship security plan and the translation (if applicable). The recognized security organization shall not be involved with the preparation of the security plan concerned or carrying out of the ship security assessment, based on which the ship security plan was prepared.
- (4) The Estonian Transport Administration will issue a “Ship Security Plan Approval Letter” and it shall be available on board together with the International Ship Security Certificate (or the Interim International Ship Security Certificate).
- (5) If the company wants to introduce changes or amendments to the ship security plan (or to any security equipment specified in the approved plan), then certain provisions in the plan (relating to section 9.4 part A of the ISPS Code) will have to be approved prior to implementation.

Relevant clauses from section 9.4:

- 1) A/9.4.2- identification of the restricted areas and measures for the prevention of unauthorized access to them;
- 2) A/9.4.4- procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;
- 3) A/9.4.5- procedures for responding to any security instructions Contracting Governments may give at security level 3;
- 4) A/9.4.7- duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;
- 5) A/9.4.15- procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;

6) A/9.4.17- identification of the locations where the ship security alert system activation points are provided; and

7) A/9.4.18- procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.

(6) Parts of ship security plan which are not described in clause 5 of this Annex do not require approval before implementation, but the company can submit those for review.

(7) Review and approval of changes or amendments to the ship security plan shall be handled as described in clauses 1 to 3 in this Annex. The Estonian Transport Administration will issue a letter “Approval of changes and amendments to the Ship Security Plan” and it shall be available on board together with the International Ship Security Certificate (or the Interim International Ship Security Certificate) and the initial “Ship Security Plan Approval Letter”.

(8) Activities listed in section 10 of Part A of the ISPS Code shall be documented (taking account of the language requirements in clause 2 of this Annex) and the relevant records maintained. On ships flying the Estonian flag at least the last 10 records of such activity shall be kept on board.

(9) Ships are required to have security incident reporting systems in place, which must be detailed in the ship security plan. These systems must cover aspects of incident reporting:

- 1) enabling shipboard personnel to report security incidents to the ship security officer;
- 2) enabling ship security officers and company security officers to report security incidents to the port facility security officer, to the Estonian Transport Administration and other relevant authorities (e.g. Estonian Police and Border Guard Board, Estonian Rescue Board).