Issued
27 October 2020
Reference
TSG 2020-8789
Applicable from
1 November 2020
Version
03.00

Swedish requirements and instructions for ship and port facility security – ISPS

Version	Date	Description	Editor
01.00	2020-09-24	New requirements and instructions issued	Maria Sakari
02.00	2020-10-19	Editorial changes and clarifications	Maria Sakari
03.00	2020-10-26	Section 4.3, editorial changes Section 7 (first paragraph), editorial changes Section 11 (new second paragraph), additional instructions	Maria Sakari

National and Union rule reference

- Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security
- SOLAS Ch XI-2
- Ship and Port Facility Security Act (2004:487)
- Ship and Port Facility Security Ordinance (2004:283)
- Swedish Maritime Administrations regulations (SJÖFS 2004:13) on Ship and Port Facility Security

Focal Point for Maritime Security

Mr Dan Sarenius

Dan.Sarenius@transportstyrelsen.se

+46 10 495 33 48 ***or*** +46 767 211 058 ***or*** +46 771 503 503

Duty Officer 365/24/7
+46 77 152 00 52

Contact Point for reporting and communication

Mrs Maria Sakari

ro@transportstyrelsen.se

+46 10 495 31 16 ***or*** +46 767 211 497

1. Mandatory paragraphs of part B of the ISPS Code

Swedish ships shall conform to the following paragraphs of Part B of the ISPS Code as if they were mandatory:

— 1.12 (revision of ship security plans),
— 4.1 (protection of the confidentiality of security plans and assessments),
— 4.4 (recognised security organisations),
— 4.5 (minimum competencies of recognised security organisations),
— 4.8 (setting the security level),
— 4.18 (identification documents),
— 4.24 (ships' application of the security measures recommended by the State in whose territorial waters they are sailing),
— 4.28 (manning level),
— 4.41 (communication of information when entry into port is denied or the ship is expelled from port),
— 4.45 (ships from a State which is not party to the Convention),
— 6.1 (company's obligation to provide the master with information on the ship's operators),
— 8.3 to 8.10 (minimum standards for the ship security assessment),
— 9.2 (minimum standards for the ship security plan),
— 9.4 (independence of recognised security organisations),
— 13.6 and 13.7 (frequency of security drills and exercises for ships' crews and for company and ship security officers).

(Article 3.5 of EU regulation 725/2004)

2. Reporting

2.1 General instructions

Where the ship is found not to be in accordance with the specifications of the ISSC and the SSP, the RSO surveyor concerned shall make sure that the necessary corrective actions are taken immediately to rectify the deficiencies.

The RSO surveyor shall inform the STA if the corrective actions are not taken or the relevant certificates are to be withdrawn.

If the ship is at a foreign port, Port State authorities shall be informed immediately.

2.2 System for control of identity of surveyors

The RSO shall provide the STA with a 365/24/7 contact point for verification of a RSO surveyor authorisation/identity.

2.3 Special reporting requirements

Security Level in Sweden
The Swedish National Police is the responsible authority for determining the security level of the ISPS Code in Swedish waters and on board Swedish ships. In urgent cases the Swedish National Police can determine the security level without communication with the STA. The STA will communicate any known changes in the security levels to the company, ship and RSO.

Only the Contracting Government have authorisation to raise or lower security levels. The Master/SSO may, when he/she finds it needed, implement the measures described in the SSP, but never officially raise the security level by himself/herself on board the vessel and document a security raise in the records. Implementation of additional security measures from the SSP should only be recorded in the deck logbook.

The RSO shall inform the STA of all information concerning changes in security level determined by the Swedish National Police which the RSO receive from the ship owner.

Security incidents
The RSO has to inform the STA of all communications concerning security incidents between the company and to the RSO.

Changes of CSO
The RSO has to inform the STA of changes in CSO identity and contact details.

3. Interim Certification

The company must submit an application for interim certification to the STA before an interim verification required by ISPS Code Part A 19.4.2 can be carried out on board.

The RSO shall in such case carry out an interim verification and send a statement to the STA verifying that

1. the ship security assessment has been completed,
2. a copy of the ship security plan meeting the requirements is provided on board, has been submitted for review and approval, and is being implemented on the ship;
3. the ship is provided with a ship security alert system meeting the requirements of regulation SOLAS XI-2/6,
4. the CSO has ensured:

   a. the review of the ship security plan for compliance with the requirements;

   b. that the plan has been submitted for approval; and

   c. that the plan is being implemented on the ship; and

5. the CSO has established the necessary arrangements, including arrangements for drills, exercises and internal audits, through which the company security officer is satisfied that the ship will successfully complete the required verification in accordance with section ISPS Code Part A 19.1.1.1, within 6 months;

6. arrangements have been made for carrying out the required verifications under section ISPS Code Part A 19.1.1.1;

7. the master, the ship security officer and other ship's personnel with specific security duties are familiar with their duties and responsibilities, and with the relevant provisions of the ship security plan placed on board; and have been provided such information in the working language of the ship's personnel or languages understood by them.

8. the ship security officer (SSO) meets the requirements.

The STA will issue an IISSC, valid for 6 months when receiving the statement from the RSO. The SSP may not be approved before an interim ISSC is issued.

In case of change of flag to Sweden the STA will determine if an interim process is required or an additional verification is sufficient.

4. Verification

4.1 Initial verification

The Ship Security Plan must be approved by the RSO (or the STA) before the Initial Verification required by ISPS Code Part A 19.1.1.1 can be carried out.

4.2 Intermediate and renewal verification

Intermediate and renewal verification is to be carried out by the RSO.

4.3 Additional verification

ISPS code defines that additional verifications shall be performed as determined by the Administration. The STA has defined the following criteria for when an additional verification shall be performed by the RSO on behalf of the flag; as a follow up on:

- port state control/detentions,
- sub-standard audit results (after corrective actions already being implemented).

The scope for such verifications should be based on the findings (with its root causes) from the port state control/detention and/or audit results.

The RSO shall without undue delay inform the STA by e-mail about all additional verifications carried out on Swedish flagged ships.

5. Approval of SSP

5.1 General

SSP may not be approved before an interim ISSC is issued.

When the RSO approve a new SSP, a copy of the approved SSP together with the associated SSA shall be sent to the STA, including a letter of approval. The documentation shall be sent by registered/tracked mail to the inspectorate office in Stockholm without undue delay. Address: The Swedish Transport Agency, Sjöfart, Box 1299, 164 29 KISTA, SWEDEN.

Approval of a new SSP or re-approval due to amendments to an existing SSP shall be followed by an issuance of a new ISSC.

5.2 Amendments requiring a new approval

The following amendments to an existing SSP requires a new approval before being implemented on board:

1. changes affecting the scope of the protective measures specified in the original SSP.
2. changes when the original SSP no longer describes normal operation.
3. changes of equipment described in the SSP.
4. changes of CSO, name and contact details.

(16 § SJÖFS 2004:13)

Following amendments may require a new approval of the SSP.

1. changes in work/rest schedules.
2. changes in crew that affects the safety/security organisation
3. changes in the working language on board
4. changes in the ship security assessment
5. new type of ship security equipment.

6. the ship implements an alternative or equivalent security arrangement
   7. changes of the ships operation,
7. the ship is rebuild,
8. changes in the ship security equipment
9. changes in areas of operation

(General advice to 16 § SJÖFS 2004:13)

5.3 Amendments implemented without prior approval

The following amendments and minor changes to the SSP may be implemented without prior approval by the RSO:

1. changes to telephone numbers
2. changes to names
3. changes to addresses
4. changes to, and updating of, existing ISM documents already approved in the Annex as a part of the SSP
5. changes to the format of checklists (records)

These amendments will be reviewed during the following ISPS Verification carried out on board the ship. (ISPS Code Part A 9.5 / 16 § SJÖFS 2004:13)

5.4 Working language

The SSP and the records of activities addressed in the SSP shall be in the working language(s) of the ship. If that working language is not English (e.g. Swedish) then a translation into English shall be provided and maintained. Both plans shall be stamped and approved by the RSO.

6. Deficiencies on board

6.1 Acceptable measures

The ISPS code does not include any possibilities for vessels to sail with open deficiencies. The STA requires anyone performing verifications (interim, initial, intermediate, additional and/or renewal) on behalf of Sweden to ensure that immediate actions are implemented, if deficiencies are observed during a verification.

The non-conformity shall be listed in the verification/survey report for the Company to further address, together with a summary of the immediate actions implemented.

Deficiencies and non-fulfilment of specified requirements (SSP, regulations, etc.) shall under no circumstances be listed as observations, notes, recommendations, room for improvement or other term if they are clearly a deficiency/non-conformity.

6.2 Issuance and endorsement of certificates

Certificates may not be issued or endorsed on board a vessel with non-conformities that has not been rectified with a corrective action.

6.3 Report to the STA

The RSO shall notify the STA of any ISPS-related deficiency found on Swedish vessels, and without delay provide the STA with a copy of the relevant verification report and accompanying corrective action plan.

Furthermore, the RSO shall without delay provide the STA with confirmation when deficiencies are closed.

When relevant, the confirmation on closed deficiencies shall include information on any equivalent measures effectuated for the audited ship.

If the ship is not able to implement any corrective actions while the RSO is on board, the ISSC should be withdrawn. The STA shall be notified about any such actions.

7. Frequency of searches

The ISPS code defines that the SSP should identify the frequency of searches of visitors, baggage and cargo.

On security level 1, SSP must identify a higher value than 0%. In order to demonstrate that these requirements are met, ship must be presented with guidance on how to document such searches, and what to look for.

For security level 2, the searches must be done on at least one person/item if cargo/storage/persons taken on board is higher than on security level 1.

8. Alternative/Equivalent arrangement (R11/R12)

The RSO are not authorised to approve alternative and equivalent security arrangements according to regulation 11 and 12. These matters must be approved by the STA.

9. Lay-up

9.1 Watch keeping arrangement

With regard to the security of laid-up ships, it is a precondition that the ship has been satisfactorily secured against unauthorised access. This means that the ship shall have a watch keeping arrangement that ensures that unauthorised persons cannot gain access on board, and that any visitors are logged with time and duration of visit.

9.2 Consequences for the ISSC

Depending on the period of the lay-up a new verification may be required.

Lay-up period up to 3 months
No consequences apart from the requirement to do a thorough search of the ship prior to departure in order to uncover any irregular conditions on board. The ship may sail with its original ISSC.

Lay-up period from 3 to 6 months
In addition to the thorough search of the ship prior to departure, a physical verification audit shall be carried out on board the ship by the RSO. The purpose of the verification is to confirm that no changes have been made on board during the lay-up period that are in conflict with the ship's security plan, and that the technical equipment included in safety measures are found on board and are in working order.

Lay-up period of more than 6 months
The ship must be subjected to a new interim certification pursuant to the current regulations unless exceptional circumstances indicate that an exemption should be granted. Exemptions may be granted following a written application by the company to the STA.

10. SSAS

10.1 General requirements

SOLAS II-2/6 requires that the SSAS equipment on board initiates and transmits a security alert to a competent authority designated by the Administration. For Swedish ships this “competent authority” is the JRCC and the company itself.

If an SSAS is not installed, approved, in working condition or alternative security measures approved by the flag are implemented when a verification is performed, the ISSC should be revoked.

The RSO surveyor has to inform STA on changes he or she becomes aware of to the SSAS including activation points, type of system or process related to sending/receiving alerts.

10.2 First Approval of SSAS

To ensure the functionality of the system, a live alert shall be submitted to JRCC in Sweden after the installation is completed. A statement of compliance of the requirements according to regulation 6 in 725/2004/EC regarding the SSAS shall be sent to the STA.

The same procedure applies if any major changes are made to the system’s set-up.

10.3 Periodical testing of SSAS

A live alert shall be submitted during the periodic survey of the radio installation or during an ISPS audit. The test should be carried out by the RSO surveyor.

Before the test, the following steps must be carried out:

1. Contact JRCC by phone (+)[1] immediately prior to testing, in order to get JRCC approval to carry out the test.
2. The identity of the surveyor will be checked.
3. Give JRCC information;
    i. Ships name
    ii. Call sign, MMSI number
    iii. Date and time for the test
    iv. Position, course and speed of the ship

After activating the SSAS, the surveyor has to call back to JRCC to confirm reception of the alert.

In case of unintentional activation of the SSAS, JRCC must be contacted immediately, see 1.

Please observe that internal test alerts shall not be sent to JRCC.

10.4 Documentation

Both the annual live alert test and the internal test of the SSAS shall be documented on board, in the ISPS security records.

Providing the vessel's SSAS test can be documented "live" with satisfactory results at the latest radio survey, the SSAS is not required to be tested "live" again at the next ISPS audit.

10.5 Malfunction of SSAS

If an SSAS is not in working condition the company has to contact the RSO and the STA for approval of alternative security measures.

[1] Note that this number may only be used for RSO internal communication.

11. Confidentiality of SSP, SSA and records

When assessing the RSO fulfilment of the ISPS Code Part A & B, regulations 4.5.5 and 4.5.6, the STA will expect RSO to maintain policies and procedures equivalent to EU "Restricted" to maintain the confidentiality of the SSP, SSA and records. (24 § SJÖFS 2004:13)

The Port State Control may request to inspect areas of a SSP. Only the STA may decide if parts relating to certain confidential information may be subject to inspection during a Port State Control. The RSO is not authorised in this matter and any questions related to disclosure of a SSP shall be sent to the STA Duty Officer.

12. Extension, suspension, withdrawal and reinstatement of certificates

If an ISPS verification is overdue, the ISSC is considered invalid. The company has to start a new certification process in order to obtain a valid ISSC again. The STA may accept companies to request initial verifications directly, if their previous certificate was a full term one. The STA must be contacted and approve such a reinstatement of an ISSC certificate.

The STA shall be notified about all ISPS verifications that becomes overdue, in order to withdraw/invalidate the ISSC, and to evaluate if the RSO should be instructed to perform an additional DOC audit.

13. Records

A Swedish ship shall keep all Declaration of Security (DOS) on board for a period of three years. DOS for the last ten port of calls shall always be available on board. (13 § SJÖFS 2004:13)

A Swedish ship shall keep all records on board for at least a period of three years. (EU regulation 725/2004, R10 app II / 36 § SJÖFS 2004:13)