REPUBLIC of SAN MARINO
MARITIME AUTHORITY

MAIN CONTACT: SAN MARINO SHIP REGISTER
PH: +378 (0549) 960075| FAX: +378 (0549) 941305| EMAIL: security@smsr.sm

Rev. 0

San Marino Policy Letter

SMPL – 2025-SEC-007

1 September 2025

San Marino Ship Register SMSR

Maritime Security

Providing information and guidance on requirements for compliance with the International Code for Security of Ships and Port Facilities (ISPS Code).

TO: Recognised Security Organisations, Companies, Owners, Company Security Officers, Deputy Company Security Officers, Masters, Ship Security Officers and the general public.

Rev. No.	Date	Changes	Initials
0	1 September 2025	1st issue	EdR

1. Preamble

The Republic of San Marino is Member state of the International Maritime Organization (IMO) since March 2002.
According to law No. 120 on the 2nd of August 2019, the San Marino Civil Aviation and Maritime Navigation Authority is acting as the maritime Administration and is supported by the San Marino Ship Register.

On the 9th of April 2021, the Republic of San Marino signed the instrument of accession, amongst the others, to the International Convention for the Safety of Life at Sea (SOLAS), 1974 as amended.

On the 26th of May 2021 the San Marino Civil Aviation and Maritime Navigation Authority adopted the Large Yacht Safety Code (LYSC) which considers the application of the SOLAS Chapter XI-2 "Special measures to enhance maritime security" and the "International Code for the Security of Ships and Port Facilities" (ISPS Code) also to all commercial yachts ≥ 24 meters in load line length and ≥ 500 GT and above engaged in international voyages.

2. Acronyms & definitions

- **Administration:** the San Marino Civil Aviation and Maritime Navigation Authority (SM CAA - MNA)
- **Company**: as defined by SOLAS regulation IX/1.2
- **CSO**: Company Security Officer, as defined by ISPS Code section A/2.1.7
- **DCSO**: Deputy Company Security Officer as identified in paragraph 4.1 of the San Marino Policy Letter SMPL-2021-SEC-014 dated 11 October 2021
- **LYSC**: Large Yacht Safety Code, SMPL-2021-TEC-008
- **Major non conformity**: as defined by the ISM Code section 1.1.10
- **Non conformity**: as defined by the ISM Code section 1.1.9
- **RSO:** Recognised Security Organisation, as defined by SOLAS regulation XI-2/1.16
- **Security incident**: as defined by SOLAS regulation XI-2/1.13
- **SMSR**: the San Marino Ship Register
- **SSP**: Ship Security Plan, as defined by ISPS Code section A/2.1.4 .

3. Scope

The scope of this policy letter is providing further information and guidance concerning the San Marino Administration requirements for compliance with the International Code for the Security of Ships and of Port Facilities (ISPS Code). It also contains the Administration's policies and interpretations regarding application and implementation of the ISPS Code, which complement those already provided by the following San Marino Policy Letters (SMPLs):

1. SMPL-2021-SEC-014 dated 11 October 2021[1]

2. SMPL-2023-SEC-004 dated 9 May 2023[2]

3. SMPL-2025-SEC-002 dated 6 February 2025[3]

4. Application

This SMPL applies:

1. to all ships listed in SOLAS Reg. XI-2/2.1.1

2. to all commercial yachts of 500GT and above engaged in international voyages (Art. 15 of the San Marino Large Yacht Safety Code)[4].

5. Additional responsibilities of Masters and Ship Security Officers

Any failure of security equipment or system, or suspension of a security measure that may compromise the ship's ability to operate at security levels 1 to 3 shall be reported without undue delay to the Company Security Officer (CSO), which will act upon.

6. Additional responsibilities of Companies

1. The Company shall maintain a proper communication with the relevant Recognized Security Organizations (RSOs) to carry out all the ISPS verifications during the established windows of the ISPS Code Section A/ 19.

2. If, for a special circumstance, the ISPS verifications cannot be completed within the established windows in the ISPS Code Section A/19, the Company shall contact in due time the RSO. If the RSO agrees on the validity of the reasons preventing the execution of the verification, it informs the Administration prior to the expiration of the relevant security certificate.

7. Additional responsibilities of Company Security Officers

1. The Company Security Officer is the direct contact point between the Company, the Recognised Security Organisation and the Administration in matters related to the ISPS Code. In case of changes of the CSO and/or the Deputy CSO (DCSO), the relevant Ship Security Plans shall be amended accordingly. Those changes shall be notified both to the RSO and the Administration.

2. The CSO/DCSO shall ensure that Ship Security Alert System apparatus on board ships under his responsibility is installed, programmed, configured and managed taking into consideration also section 4.1 of the SMPL-2021-SEC-014.

3. Failures of security equipment or system, or suspension of a security measure that may compromise the ship's ability to operate at security levels 1 to 3 shall be addressed by the Company Security Officer which will act upon in consultation with the RSO.

---

[1] https://www.smsr.sm/wp-content/uploads/2023/03/211011-SMPL-2021-SEC-014-Maritime-Security.pdf
[2] https://www.smsr.sm/wp-content/uploads/2023/05/04-SMPL-2023-SEC-004.pdf
[3] https://www.smsr.sm/wp-content/uploads/2025/02/250206-SMPL-2025-SEC-002.pdf
[4] https://www.smsr.sm/wp-content/uploads/2023/03/210526-SMPL-2021-TEC-008-LYSC-1.pdf

For these failures, the CSO shall provide the RSO with:

1. Details of the major failures identified, and measures adopted to solve the problem or to downgrade the failure and, in such last case, details of the proposed corrective measure the ship will apply until the failure is rectified
2. An action plan specifying the timing of any repair or replacement and a risk assessment.

4. In compliance with SMPL-2025-SEC-002 dated 6 February 2025, the CSO is required to provide SMSR with assurance of the received information on the Security Level 3 or 2 adopted by the Administration and their application on board the ships concerned.

8. Additional responsibilities of Recognised Security Organisations

1. The Recognised Security Organisations acting on behalf of the San Marino Administration shall maintain a proper communication with the Company and ensure to make all the necessary arrangements to complete all the ISPS verifications during the established windows set in the ISPS Section A/19. RSOs shall also follow the instructions provided with SMPL-2023-SEC-004.

2. All RSOs before approving/reviewing Ship Security Plans shall check that such plans are coherent with requirements of the mandatory part of the ISPS Code as well as provisions set in the SMPLs referred to in paragraph 3. (Scope) of this document.

3. Following consultation with the Administration and in compliance with provisions of the ISPS Code Sections A/19.4.1 to A/19.4.5, the RSO may issue an Interim International Ship Security Certificate (Interim ISSC). The Interim ISSC is valid for six (6) months or until the ISSC is issued, whichever comes first. The RSO shall re-issue the Interim ISSC with the same validity as the existing certificate if the ship changes any of the following data:
   1. When the name of the ship changes
   2. When the tonnage of the ship changes
   3. When the name and/or the physical address of the Company change
   4. When the type of the ship changes.

   The Interim ISSC cannot be extended. Except for the cases listed above (Points 8.3.1. to 8.3.4.) RSOs shall refrain from issuing a consecutive Interim ISSC. However, if the RSO is convinced of the good faith of the ship and the Company, and believes that the purpose of the request for a subsequent, consecutive Interim ISSC does not hide the scope to circumvent full compliance with SOLAS Chapter XI-2 and Part A of the ISPS Code, it may seek the authorization of the Administration for issuing a subsequent, consecutive Interim ISSC. In such a case the RSO shall provide SMSR the following:
   5. Details of the circumstance
   6. An action plan specifying the time schedule and the related risk assessment.

4. At request of the RSO, in exceptional cases that do not represent a danger to the ship or persons on board and without presenting an unreasonable threat of harm to the environment, the San Marino Ship Register (SMSR) on a case-by-case basis, following consultation with the Administration and in compliance with Article 8.4 of the SMPL-2023-SEC-004, may authorise the RSO to issue an ISSC whit a shorter validity than that used for a “Full Term” ISSC.

The RSO shall provide the SMSR with:

1. Details of the exceptional circumstances
2. An action plan specifying the time schedule, details of the temporary equivalent measures the ship will adopt until the non-conformity is rectified, and the related risk assessment.

This certificate shall be identified by the nomenclature “Short Term” International Ship Security Certificate, and its validity should not exceed one (1) month. When a Short Term ISSC is issued by the RSO according to its internal rules, it shall be notified to SMSR.

5. For each verification conducted according to Section A/19.1 of the ISPS Code the RSO shall draft a report. Such report should include at least the following information:
   1. Type of verification (Interim, initial, intermediate, renewal, additional)
   2. Ship’s and Company data
   3. Place and date of the verification
   4. CSO and SSO data
   5. Identification of the audit team
   6. The status of the implementation of the SSP
   7. Confirmation on the operational status of all security equipment and systems on board
   8. Details of any failures found during the verifications
   9. Any instruction or observation made and possible required actions
   10. Recommendations
   11. Conclusion

   This list complements that already provided in paragraph 10.4 of the SMPL-2023-SEC-004 dated 9 May 2023. At request, the report shall be shared with the SMSR.

6. If during a ship’s ISPS verification, the RSO found a mayor non conformity, which can compromise the security of the ship, cargo or persons, this shall be documented and reported without delay to the CSO. Immediate action is required to restore compliance and the major non conformity must be solved or, at least, downgraded before departure. RSO shall notify SMSR the following:
   1. Details of the major non conformity identified and activity done to restore compliance or, at least, to downgrade it to a non conformity
   2. In case of downgrading, details of the temporary equivalent measure the ship has adopted and will maintain until the non conformity is rectified and an action plan specifying the timing of any repair or replacement which should not exceed three (3) months.

7. Additional verifications in accordance with ISPS Section 19.1.1.3 may be carried out at request of the Administration, Port State Control Authority, and on the initiative of the RSO in consultation with SMSR.

9. Certifications for ships resuming service after a laid-up period

In accordance with Annex 1 of the SMPL-2023-SEC-004 dated 9 May 2023:

1. If the ship is out of service between three (3) and (6) months, an additional verification shall be done. The ISSC shall be endorsed as appropriate

2. If the ship is out of service more than (6) months, an interim verification as required

by ISPS Section A/19.4.2 shall be done. An Interim ISSC shall be issued as appropriate.

These instructions do not apply to ship for which seasonal lay-ups are normal part of their operational routine.

10. Invalidation of the maritime security related certificates

An existing ISSC certificate shall be considered invalid in, but not limited to, the following circumstances:

1. When a ship has not undergone the periodical or additional verifications (Intermediate, renewal and additional verification)
2. When a Company ceases managing the ship
3. When a ship changes its flag
4. When an ISSC (“Full Term”, Interim ISSC, “Short Term”) is issued to replace another ISSC
5. When a part of the Ship Security Plan (SSP) which requires approval upon amendment has been amended without approval
6. When corrective actions for non compliance set out at verifications have not been completed within the established period of time
7. When a ship is not operated in compliance with rule requirements
8. When the ship fails to maintain its SSP in compliance with the requirements of the ISPS Code
9. Any other notification of invalidation made by the Administration or the RSO.

11. Entry into force

This SMPL shall enter into force and shall apply from 15 September 2025.

End of the document