SAFESEANET

Interface and Functionalities Control Document

SSN IFCD

Version: 1.4

Date: 2 July 2025

Document Approval

	Name	Date	Signature
Prepared by:	EMSA	13-05-2025	
Checked by:	SSN/LRIT Group	27-05-2025	
Quality control by:			
Approved by:	HLSG	02-07-2025	

Distribution List

Company	Name	Function	For Info / Approval
/	/	/	/

Change Control History

Version	Date	Last approval	Description
1.00	13-12-2010	HLSG	First version approved
1.1.0	23-06-2014	HLSG	Updates regarding Directive 2010/65/EU implementation and reference to the streaming mechanism for data distribution. with the exception of: 1) chapter 2.6, Cooperation with Other EU Systems, which will be revised in order to include the interface between SSN and CECIS, as approved by HLSG; and 2) chapter 3.4 Maximum access rights per role, which will be revised to adjust the matrix of access rights (Table 2).
1.1.1	02-12-2014	HLSG	Updates requested at 11th HLSG meeting: 1) chapter 2.6, Cooperation with Other EU Systems - interface between SSN and CECIS 2) chapter 3.4 Maximum access rights per role – data stream 3) chapter 3.5, Access to SSN incident reports by CECIS users
1.1.2	07-07-2016	HLSG	Amendments linked to the revision of the VTMIS Directive as per Directive 2014/100/EC
1.2	28-02-2018	HLSG	Simplification of access rights
1.3	08-12-2022	HLSG	Updates regarding Directive 98/41/EC as amended and Directive EU 2019/883
1.4	02-07-2025	HLSG	Use of SSN data by shipping industry and 3rd countries for the purpose of reporting MRS – data reuse Access for other organisations to submit Incident Reports with an operational benefit

Table of Contents

Summary of Amendments

Page	Map/block text	Description of changes	Rationale	Approval date
IFCD v 1.4				
44	Chapter 3.7	Access for users from the shipping industry	HLSG 15	02-07-2025
45	Chapter 3.8	Access by non-SSN participating countries for reporting MRS	As above	02-07-2025
47	Chapter 3.9	Access for other organisations to submit Incident Reports with an operational benefit	As above	02-07-2025
IFCD v 1.3				
13	Chapter 1.4	New definitions and amendment to existing ones	HLSG 11	08-12-2022
22	Chapter 2.3	Amendments to the exchange of information via SSN	As above	08-12-2022
24	Chapter 2.4	Amendments to the additional system functionalities	As above	08-12-2022
28-29 31-32	Chapter 2.5	Amendments to the streaming interface and new Integrated Reports Distribution mechanisms	As above	08-12-2022
32, 34	Chapter 2.6	Inclusion of cooperation with THETIS-EU	As above	08-12-2022
38-39	Chapter 3.3	Amendments to the definition of roles. New role for the AIS Regional Server	As above	08-12-2022
41-43	Chapter 3.4	Amendments to the access rights matrix	As above	08-12-2022
49	Chapter 5.2	Amendments to the System Support Services at National Level	As above	08-12-2022
52	Chapter 5.3	Deletion of the SHT early warning	As above	08-12-2022
57-60	Chapter 7.2	Amendments in line with the additional security measures from the SSN Security Guidelines	As above	08-12-2022
IFCD v 1.2				
12-18	Chapter 1.4	New definitions and amendment to existing ones	HLSG 2 approval to simplify the access rights policy	28-02-2018

Page	Map/block text	Description of changes	Rationale	Approval date
19-21	Chapter 1.6	Amendment to SSN/LRIT group and IMS group definitions	As above	28-02-2018
24	Chapter 2.4	Amendments to sub-chapters on the IMS functionalities	As above	28-02-2018
25	Chapter 2.5	Amendment of Figure 2, update of the information exchange mechanism	As above	28-02-2018
31-33	Chapter 2.6	Amendments to reflect the cooperation with Earth Observation Data Centre and other systems	As above	28-02-2018
34-42	Chapter 3	Amendments in line with the simplification of access rights	As above	28-02-2018
IFCD v 1.1.2				
8	Background	Amendments in line with the new Annex III.	Dir. 2002/59/EC Annex III amendment stemming from Dir.2014/100 /EC	07-07-2016
10	Chapter 1.1 and 1.2	Inclusion of Integration of data and Integrated Maritime Services (IMS)	As above	07-07-2016
11 to 16	Chapter 1.4	New definitions and amendment to existing ones	As above	07-07-2016
17 to 19	Chapter 1.6	Clarification to the SafeSeaNet group definition. Definition of the IMS group	As above	07-07-2016
19	Chapter 1.7	Reference to IMS in SSN technical and operational documentation	As above	07-07-2016
21-22	Chapter 2.2	Amendments in line with the new Annex III.	As above	07-07-2016
23	Chapter 2.4	Creation of sub-chapters to integrate the IMS functionalities	As above	07-07-2016
25 to 27	Chapter 2.5	Amendment of Figure 2, update of the information exchange mechanism	As Above and to reflect the possibilities offered by IMS	07-07-2016
30-31	Chapter 2.6	To reflect the amended legal background of CECIS and the cooperation with other systems for IMS	To identify the exchange already in place	07-07-2016

Page	Map/block text	Description of changes	Rationale	Approval date
32	Chapter 3.1	Amendments in line with the new Annex III. Precision on access rights.	Dir. 2002/59/EC Annex III amendment stemming from Dir.2014/100 /EC	07-07-2016
33	Chapter 3.2	Reference to the IMS Point of Contact (PoC) and to the role of Central SSN administrator and National IMS administrator	To identify the bodies responsible to assign IMS access rights	07-07-2016
33 to 35	Chapter 3.3	Identification of the roles Mandatory System Functionalities and for IMS functionalities	To identify the roles involved in SSN functionalities	07-07-2016
35 to 38	Chapter 3.4	Clarification and identification of access rights for IMS users. Simplification of the access rights matrix.	To support the notion of integration, a need for simplification was identified	07-07-2016
39	Chapter 3.5 and 3.6	Clarification and editorial changes	/	07-07-2016
40-41	Chapter 4.1, 4.2 and 4.3	Mention IMS, the performance and the operational coordination applying to them	/	07-07-2016
43 to 45	Chapter 5.1, 5.2	Amendments to reflect the IMS	To reference IMS in the various paragraph when required	07-07-2016
47	Chapter 5.3	Add IMS specific procedure	To include IMS procedure to existing procedures	07-07-2016
49	Chapter 6.1	New paragraph (6.1.3) related to the change management for IMS functionalities	/	07-07-2016
IFCD v1.1.1:				
29	Chapter 2.5.2	Inclusion of the data distribution process		02-12-2014

Page	Map/block text	Description of changes	Rationale	Approval date
34	Chapter 2.6	Interface between SSN and CECIS	Updates regarding HLSG 11	
40	Chapter 3.4	Inclusion of the data distribution process – Access rights		
46	Chapter 3.5	Interface between SSN and CECIS		
IFCD v1.1.0:				
6	Background	Updates regarding Directive 2010/65/EU	Updates regarding Directive 2010/65/EU	23-06-2014
14	Chapter 1.4	Definition of NSW and LOCODES added		
24	Chapter 2.2	Exchange of information from the notification of waste and residues and the notification of security information		
25	Chapter 2.3			
26	Chapter 2.3	Management of information on exemptions		
29	Chapter 2.5.2 and 2.5.3	Inclusion of the streaming mechanism for data distribution	Pilot project outcome	
39	Chapter 3.3	Inclusion of the "National Single Window" role and its access rights	Updates regarding Directive 2010/65/EU	
39	Chapter 3.3	Inclusion of the "Waste" and "Security" roles and their access rights		
52 55	Chapter 5.2 and 5.3	Management of information on exemptions		
52 55	Chapter 5.2 and 5.3	Coastal stations and Places of Refuge Information	Update regarding HLSG 9	
62	Chapter 7.2.2.5	Update Commercial Sensitive information with cargo residues	Updates regarding Directive 2010/65/EU	

Background

Following the accident involving the crude oil tanker *ERIKA* off the French coast in 1999, the European Union adopted several legal instruments for improving the prevention of accidents at sea and combating marine pollution. Directive 2002/59/EC of the European Parliament and Council of 27 June 2002 as amended, establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC, and within that Directive (Annex III) established the Union Maritime Information and Exchange system "with a view to enhancing the safety and efficiency of maritime traffic, improving the response of authorities to incidents, accidents or potentially dangerous situations at sea, including search and rescue operations, and contributing to a better prevention and detection of pollution by ships." Member States (MS) and the European Commission shall cooperate in the development of a computerised data exchange system and its necessary infrastructure.

To achieve these objectives, in 2001, the European Commission launched the development of a European network called SafeSeaNet. The main objective of SafeSeaNet is to provide a European platform for maritime data exchange between maritime administrations in the Member States to ensure the implementation of Union legislation in the area of vessel traffic monitoring. It comprises a network of national SafeSeaNet systems in Member States and a central SafeSeaNet system acting as a nodal point, which interacts with the national systems.

Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC enhances the role of SafeSeaNet in facilitating the reception, exchange and distribution of information between the information systems of Member States on maritime activity. In accordance with this Directive, Member States shall ensure that information received from reporting formalities provided in a legal act of the Union is made available in their national SafeSeaNet systems and shall make relevant parts of such information available to other Member States via the SafeSeaNet system. In addition it provides that to facilitate maritime transport and to reduce the administrative burdens for maritime transport, the SafeSeaNet system should be interoperable with other systems of the Union for reporting formalities.

This legal framework requires the collection and distribution of various kinds of data regarding vessel traffic monitoring, port call information, dangerous and polluting cargo details, bunkers, security, waste and cargo residues, persons on board passenger ships, incidents and accidents reports. SafeSeaNet is established to facilitate this exchange of information in an electronic format. The European Maritime Safety Agency, in cooperation with the Member States and the Commission is responsible for: the technical implementation and the documentation of the Central SafeSeaNet system; the development, operation and integration of the electronic messages and data as well as maintenance of the interfaces with the central SafeSeaNet system, including AIS data collected by satellite, LRIT and other information systems, as referred to in Annex III of Directive 2002/59/EC as amended.

Annex III of Directive 2002/59/EC (as amended) requires the Commission, in close collaboration with the Member States, to develop and maintain the Interface and Functionalities Control Document (IFCD).

Chapter 1 - Introduction

1.1 Primary Objectives

The purpose of the Interface and Functionalities Control Document (IFCD) is to describe in detail: the performance requirements and procedures applicable to the national and central elements of SafeSeaNet (SSN) in order to ensure compliance with the relevant Union legislation; the integration of data, and; the development, implementation and provision of Integrated Maritime Services through the SafeSeaNet system.

1.2 IFCD Overview

The IFCD is a comprehensive document describing the following elements for the SSN system:

a) the objectives, the system architecture, the types of data held, the roles and responsibilities of users, the sources and recipients, the system interfaces and the relationship with existing systems;
b) the performance requirements in terms of data handling, timing, availability and storage, the rules applicable for access rights, data transmission and exchange, and archiving at national and central level;
c) the procedures applicable to ensure data quality control, system management, testing and data security, and
d) the Integrated Maritime Service functionalities and related operational aspects.

It should be noted that some technical and operational documentation related to SSN, such as standards for data exchange formats, user manuals and network security specifications, are not an integral part of the IFCD. However, these are described in the associated SSN technical and operational documentation (please refer to Chapter 1.7), and the IFCD contains references where appropriate.

In terms of the relationship between the IFCD and SSN technical and operational documentation, the IFCD contains the high level technical and functional/operational requirements of the system, while the more detailed specifications are described in the SSN technical and operational documentation.

1.3 IFCD Structure

The Interface and Functionalities Control Document (IFCD) is structured in the following manner.

- Chapter 1 - "Introduction" includes the definition of relevant terms, information on document management policy and the roles of the parties concerned.
- Chapter 2 - "SafeSeaNet Overview" provides a system overview and outlines the architecture of the information structure and technologies used. The system functionalities and features are described in this chapter.
- Chapter 3 - "Roles and responsibilities" defines the users, their roles and the access rights applicable to data distribution.

- Chapter 4 - "SafeSeaNet Performance" describes the information flows; the services and performance rules for the messaging processes and; the information exchange systems applicable to both the national and central SSN systems.
- Chapter 5 - "Operational Services and Procedures" covers the services, operational procedures and best practices relevant to both the national SSN and central SSN systems.
- Chapter 6 - "System Management and Tests" describes the procedures applicable to the management of the SSN system; the test procedures and rules; the changes to the system's status and; the procedures for performing commissioning tests.
- Chapter 7 - "System Security" provides clarification on security related terminology and defines the rules and procedures applicable to data transmission and exchange.

Each page of the document includes the following information in its header:

- Version Number.
- Date of issue.

The list of amendments to the IFCD is recorded in the Summary of Amendments (page 5). SSN users should ensure that they use the latest version of the IFCD.

1.4 Definitions and Abbreviations

For IFCD purposes, the definitions in Article 3 of Directive 2002/59/EC, as amended, shall be applicable, as well as the following definitions and abbreviations:

Access Control – The process that ensures that resources are only granted to those users who have a need for the information and own the proper access rights.

Access Rights – The set of privileges granted to a user allowing them to have access to certain kinds of information or services.

Accountability – The process that ensures that the actions within the system of an entity may be traced uniquely to the entity.

AIS (T-AIS and SAT-AIS) - Automatic Identification System information provided by ships in accordance with the provisions of Chapter V of SOLAS, received by Member States' shore-based installations (T-AIS) and also received through detection by satellites (SAT-AIS).

AIS Regional Server – A server that a group of MSs agrees to maintain[1] in accordance with the security and reliability requirements of the SSN system. The regional server is also used for relaying AIS data from their national SSN systems to the central SSN system. The service may include data collection, storage, backup and re-distribution, as well as monitoring the availability and quality of the data. For these functionalities, and as long as the MSs concerned request to use it as an alternative to the direct connection to the central SSN system, the AIS Regional Server will be considered to be a component of the central SSN system.

[1] Under any agreement made between the MSs.

AIS Regional Server Administrator (RS Administrator) – the Authority which assumes responsibility for the AIS regional server system and its management. The RS Administrator is responsible for the maintenance and operation (on a 24/7 basis) of the existing AIS regional server, its availability and its connection to the national AIS networks of the countries participating in the AIS regional server and to the central SSN system, and for ensuring its compliance with the requirements described within the IFCD and the agreed service level in force.

Authentication – The process of determining whether someone or something is who or what it is declared to be.

Authorisation – The process of granting access rights to a user.

Central SafeSeaNet Administrator – Designated person at EMSA who assigns:

- access rights and functional roles within the boundaries defined by the data owner for the Integrated Maritime Services (IMS), as defined in Chapter 2.4.2;
- access rights and functional roles to users belonging to other EU institutions and bodies, in line with the legal framework and within the allowed maximum boundaries defined per role, for the Mandatory System Functionalities as described in Chapters 2.3 and General Additional Functionalities as defined in 2.4.1.

Central SafeSeaNet system (central SSN system) – This comprises those SSN components (both technical and procedural) which act as the central/nodal point for the exchange of information between national SSN systems.
The responsibilities related to the central SSN system are defined in paragraph 2.1.2 of the annex III of the Directive. The Central SSN system also comprises the Integrated Maritime Services component.

Classified information – Any information and material, an unauthorised disclosure of which could cause varying degrees of prejudice to EU interests, or to one or more of its Member States, whether such information originates within the EU or is received from Member States, third States or international organisations (in accordance with Commission Decision 2001/844/EC amending its internal Rules of Procedure by annexing Commission Provisions on Security).

Commercial sensitive information - Information that is likely to prejudice the commercial interest of any person (a person may be an individual, a company, the public authority or any other legal entity).

Commissioning tests – Tests which assess whether national SSN systems support the reliable, timely and accurate exchange of information within the SSN system (as defined in the MS Commissioning Tests Plan). The commissioning process covers all SSN messages transmitted to/from the central SSN system.

Confidentiality – The process that ensures that information is not made available or disclosed to unauthorized entities.

Data provider – An authorised SSN user who provides information required by the SSN legal framework to other MSs through the SSN system, and makes it available to data users, as well as an entity, which provides information or data owned by third parties, within the scope of the Integrated Maritime Services (IMS) and identified in the appropriate service agreement.

Data user – An authorised SSN user requesting: information as required by the SSN legal framework from other MSs, or; data owned by third parties within the scope of the Integrated Maritime Services (IMS) through the SSN system.

SSN Details: information available upon request to the SSN national system (e.g. Hazmat Details, Waste Details, Security Details, MRS Details etc.) ruled and managed by specific access rights.

Digital Certificate – A digitally signed statement that certifies the binding between the owner's identity information and his/her electronic public key.

Encryption – The Cryptographic transformation of data into a form that conceals the data's original meaning to prevent it from being known or used by unauthorized entities.

Earth Observation Data Centre – The EMSA Earth Observation Data Centre (EODC) entered operations in 2011 in support to the CleanSeaNet service (EMSA's satellite oil spill monitoring service). The EODC is responsible for the ingestion, processing and distribution of EO data to EMSA services that require earth observation information (i.e. CleanSeaNet, Copernicus Maritime Surveillance, Integrated Maritime Services for Member States, Integrated Maritime Services to FRONTEX, etc.). The EODC handles a wide range of EO products, from multiple satellites, and providers and delivers information derived from EO data to a wide range of user communities according to clear rules and access rights.

Earth Observation products – Earth observation products are based on information that can be acquired from Earth Observation satellites that usually have either radar or optical sensors. These products include images (the primary product) and value adding products (extracted from the image using algorithms). The value adding products used by EMSA include vessel detection, activity detection, oil spill detection, change detection and met-ocean (wind and wave from SAR).

Exchange mechanism – Constitutes the entire electronic data interchange system, including the transmission, message flow, document format, and software used to interpret the documents.

Function - allocated task and/or responsibility which requires and justifies the use of particular maritime data sets, information and functionalities, in line with the access rights and the existing legal framework. The function is independent of the governmental department/authority in which users are based and is associated to the task and/or responsibility the users are in charge of.

High Level Steering Group for Governance of the Digital Maritime System and Services (HLSG) – *(hereafter 'HLSG')* The governance group defined in Annex III of Directive 2002/59/EC (as amended), which comprises MS and Commission representatives, and which has the tasks defined in Commission Decision (EU) 2016/566 of 11 April 2016 (Repealing decision 2009/584/EC of 31 July 2009). The HLSG's tasks shall be:

(a) as stipulated in point 2.2 of Annex III of Directive 2002/59/EC;

— make recommendations to improve the effectiveness and security of the system,

— provide appropriate guidance for the development of the system,

— assist the Commission in reviewing the performance of the system,

— provide appropriate guidance for the development of the interoperable data exchange platform combining information from SafeSeaNet with information from the other information systems as referred to in point 3,

— approve the interface and functionalities control document referred to in point 2.3, and any amendments thereto,

— adopt guidelines for the collection and distribution of information through SafeSeaNet related to competent authorities designated by Member States to perform relevant functions under this Directive,

— liaise with other relevant working forums, in particular the group on maritime administrative simplification and electronic information services.

(b) to assist the Commission in the fulfilment of its tasks set out in Article 3(2) of Directive 2010/65/EU, in particular assist in developing technical mechanisms for the harmonisation and coordination of reporting formalities within the Union enhancing integration, re-use and sharing of information reported into the system, enabling reporting once and thereby supporting the facilitation of the European maritime transport space without barriers;

(c) To establish and maintain cooperation with expert group(s) for specific tasks related to the operation, use and functioning of the Union maritime information and exchange system, the national single window, the national SafeSeaNet or other electronic systems and their interoperability, under terms of reference established by the HLSG;

(d) to establish the cooperation between the Member States bodies and the Commission regarding: — Article 23 of Directive 2002/59/EC, — questions related to conditions for use of the system and the integrated maritime services;

(e) to monitor the interconnection and interoperability of the national single window and the Union maritime information and exchange system as well as other relevant European systems used for managing the information;

(f) to bring about an exchange of experience and good practice for the purposes of Article 20(3) of Directive 2002/59/EC.

Integrity – The process that ensures the accuracy and completeness of information.

Integration – capability of processing and correlating maritime data sets and information including: LRIT, Satellite-AIS, VMS, satellite remote sensing Earth Observation imagery and derived products, SSN Mandatory System Functionalities (as per chapter 2.3), as well as any other maritime-related data sets and information.

Integrated Maritime Services (IMS) – Configurable, voluntary, functionalities, promoting regional, national and local cooperation, providing an enhanced maritime picture, using the integration capability, following the agreed access rights and responding to the data users specific needs. These functionalities foster the sharing and exchange of data between different users and applications and provide additional, complementary and supportive tools. They do not replace any existing systems and mandatory system functionalities as defined in Chapter 2.3. IMS are offered to Member States, following a functional approach. They are also offered to users of several EU entities.

Integrated Maritime Services (IMS) Group - The Group, open to representatives from all MSs, the Commission and EMSA, as defined in Chapter 1.6.2, has the responsibility for managing technical and operational issues of the voluntary additional system functionalities as described in Chapter 2.4.2.

Local Competent Authority (LCA) – These are authorities or organisations designated by MSs to receive and transmit information pursuant to the SSN legal framework (e.g. port authorities, coastal stations, Vessel Traffic Services, shore-based installations responsible for a mandatory ship's routing system or a mandatory ship reporting system approved by the IMO and bodies responsible for coordinating search and rescue operations).

LOCODES – Location codes which include both UN/LOCODES and SSN Specific LOCODES as established by the NCA according to the SSN LOCODES Guidelines.

Long Range Identification and Tracking of ships (LRIT) information system – Ships for which SOLAS Chapter V reg. 19-1 apply shall be fitted with a system to automatically transmit the following information:

- Identity of the ship;
- The position of the ship (latitude and longitude);
- The date and time of the position provided; and
- The ship type.

The processing of this information for EU ships, as well as gathering this information from other LRIT Data Centres for non-EU ships, is performed by the European Union Cooperative LRIT Data Centre, and the resulting information is made available via SSN.

Maritime Support Services (MSS) – The 24/7 EMSA service responsible for monitoring the EU maritime transport operational systems (in particular SSN) for the exchange between MSs (and some participating third countries) of information on ships, their voyages, their cargoes and incidents at sea (including accidents and pollution). The MSS is permanently monitoring the data quality in, and the performance and continuity of, the operational systems. It also provides a helpdesk facility to the SSN Community and supports the prompt mobilisation of EMSA's contracted oil pollution response vessels following a MS request.

Meteorology and oceanography (METOCEAN) – Information and measurements of meteorological and oceanographic conditions, such as air temperature, surface atmospheric pressure, wind speed and direction, currents and waves.

National IMS Administrator - Designated person who creates users, assigns access rights and functional roles to the IMS users as defined in Chapter 2.4.2. and is point of contact for the monitoring and operational procedures.

National Competent Authority (NCA) – The body which assumes responsibility for a national SSN system and its management on behalf of a MS. It is responsible for the operation, verification and maintenance of the national SSN system, and for ensuring that the standards and procedures comply with the requirements described within the IFCD and with the agreed technical and operational documentation. The NCA responsibilities are defined in Annex III of Directive 2002/59/EC, as amended. For LRIT, the NCA responsibilities are defined in the Conditions of Use (CoU) signed between EMSA and EU LRIT CDC participating countries.

National SafeSeaNet Administrator – Designated person who create users, assigns access right and functional roles to National and Local users, in line with the legal framework and within the defined roles, for the Mandatory System Functionalities as defined in Chapters 2.3 and General Additional Functionalities as defined in Chapter 2.4.1.

National SafeSeaNet system (national SSN system) – This comprises technical and procedural SSN elements which support the provision, retrieval and use of information required to implement the SSN legal framework within an MS. These elements are the responsibility of the relevant MS and can be administered either directly by the NCA, via the establishment of LCAs or by setting up other appropriate arrangements with third parties.

National Single Window (NSW) – It is the single window established by Member States in accordance with Directive 2010/65/EU.

NCA 24/7 – The contact point at national level used for 24/7 operational contacts between MSs and with the EMSA MSS.

Non-repudiation – The process that ensures that the entities involved in a communication cannot deny having participated (e.g. sending entity cannot deny having sent a message).

Notification – Required information sent by the national SSN systems to the central SSN system to inform the SSN community of an event related to a vessel or an incident at sea.

Operational requirements – Requirements which focus on the operational usability of SSN, and which define the information, business rules and responsibilities that should be respected during SSN system operation. Operational requirements derive from the legal framework, as interpreted by decisions taken by the HLSG or SSN groups and recorded in SSN documentation.

Password – A string of characters used to authenticate the identity of a user. The format of passwords used in SSN is given in the SSN Technical and Operational Documents.

Personal Data – Any information relating to an identified or identifiable natural living person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number.

Point Of Contact (PoC) for Integrated Maritime Services (IMS) – The body appointed by the Member State, which is a single point of contact for the Integrated Maritime Services related matters and assumes, at national level, responsibility for: coordination of data users and, if applicable, data providers; the designation of the National IMS Administrator; the access rights coordination with the competent authorities, and user requirements coordination.

Request/response mechanism – This describes the activities to be carried out when a MS requests detailed information on a notification via SSN.

Remote Sensing Aircraft data - Data acquired by unmanned aircrafts used in maritime surveillance operations. This could include for example AIS, Emergency Position Indicating Radio Beacon (EPIRB) information, live video stream, infra-red data, optical and radar imagery, measurements of emissions and in situ data about events and objects detected at sea.

SafeSeaNet authority (SSN authority) - These are authorities defined as NCAs, LCAs and EMSA, on behalf of the European Commission for the central SSN system. This covers both "Competent authorities" and "Port authorities" as defined in Article 3 of 2002/59/EC as amended.

SafeSeaNet legal framework – All requirements which relate to SSN, as defined by the following legal instruments:

- Directive 2002/59/EC as amended (establishing a Community vessel traffic monitoring and information system);
- Directive 2019/883 (on port reception facilities for the delivery of waste from ships);
- Directive 2009/16/EC (on port State control);
- Directive 2010/65/EU (on reporting formalities for ships arriving in and/or departing from ports of the MSs) and;
- Regulation (EC) No 725/2004 (on enhancing ship and port facility security);

SafeSeaNet/LRIT Group (SSN/LRIT Group) – The working Group, which comprises representatives from MSs, Overseas Territories (LRIT), Third Countries (LRIT), the Commission and EMSA with responsibility for managing technical and operational issues relating to SSN and LRIT with tasks as defined in Chapter 1.6.1.

SafeSeaNet system (SSN system) – This comprises both the national and central SSN systems.

SafeSeaNet user (SSN user) – This refers to **a person** or **persons performing the same function and position** (e.g. duty officers on shift work within a single MRCC or VTS-centre) (i.e. an SSN Web user using a browser-based web interface at central, national or local level) or **a system** (at national level the national SSN system, and at local level the LCA systems).

Service – A mean to deliver added value to users by supporting their function(s) through dedicated mechanisms.

Ship AIS position enriched with SSN data – This information consists of Ship AIS position collected by fixed-based stations of Member States provided to the central SSN system enriched with a confirmation of the presence of voyage, Hazmat, Waste, Security, MRS and Incident Reports information provided by Member States.

System Security information - Information which requires protection as its publication or unauthorised disclosure would reveal privileged or confidential information related to persons, systems, operations and/or facilities.

S-TESTA – A private network that gives public administrations access to modern telecommunications services for daily dealings with other public sector bodies across Europe. Its purpose is to provide European institutions and agencies, as well as administrations in the MSs, with network infrastructure that ensures the easy, reliable exchange of data.

Technical requirements – The information and communication technologies (ICT) requirements which need to be taken into account when developing, updating and operating the components that make up national and central SSN systems and their interfaces. The technical requirements support the implementation of the operational requirements.

Traceability – Traceability is the process to verify the history, location, or application of the information by means of documented recorded identification.

The Union Maritime Information and Exchange System (SafeSeaNet) – *system developed by the Commission in cooperation with the Member States to ensure the implementation of Union legislation.*

Unclassified information – Information that can be released to individuals without a clearance except when it is deemed personal or sensitive.

UN/LOCODE – The United Nations Code for Trade and Transport Locations (UN/LOCODE) is an international, geographical coding scheme which has been developed and maintained by the United Nations Economic Commission for Europe (UNECE).

Vessel Monitoring System (VMS) – Satellite-based fishing vessel monitoring system providing data to fisheries authorities at regular intervals on the location, course and speed of vessels (as defined by Council Regulation (EC) No 1224/2009 of 20 November 2009 and Commission implementing regulation (EU) N°404/2011).

1.5 IFCD Administration

The High-level Steering Group (HLSG) approves the IFCD and any amendments thereto. EMSA is responsible for keeping the latest version updated (as approved by the HLSG) and for its distribution to all NCAs in electronic format. The IFCD will also be available electronically on the EMSA website.

1.6 SafeSeaNet/LRIT User Groups

1.6.1 SafeSeaNet / LRIT Group

The SSN/LRIT Group is made up of representatives of the Member States, of Overseas Territories (LRIT), of Third Countries (LRIT), of the Commission and EMSA. Representatives from other organisations and industry may be invited to participate as observers.

The objective of the SSN/LRIT Group is to manage the technical and operational issues related to the mandatory system functionalities of SSN (as defined in Chapter 2.3) and LRIT.

The NCAs are responsible for designating their representatives on the SSN/LRIT Group, and for providing their names and functions to EMSA.

EMSA chairs and is responsible for managing the SSN/LRIT Group.

The SSN/LRIT Group adopts its own rules of procedure, and these constitute part of the SSN technical and operational documentation as defined in chapter 1.7.

The SSN/LRIT Group aims to:

a) regularly report to MSs, European Commission (COM) and the HLSG on SSN activities (both central and national systems) and LRIT;

b) define user requirements, monitor the system and support its adaptation to users' requirements;

c) define the necessary modification and adaptation of the system in order that it complies with the latest regulations;

d) coordinate the network of SSN and LRIT users;

e) define new system functionalities and user interfaces as requested by the HLSG;

f) develop and update SSN technical and operational documentation, and;

g) propose amendments to the IFCD.

The SSN/LRIT Group may decide to create working groups to examine specific issues related to SSN. The general objectives and tasks given to such entities are defined in the terms of reference determined by the SSN/LRIT group. The working groups shall be dissolved as soon as their mandates are fulfilled.

The SSN/LRIT Group consults and reports to the HLSG on issues related to the HLSG mandate, as defined in Chapter 1.4 under "HLSG", or in accordance with the VTMIS Directive (2002/59/EC).

1.6.2 Integrated Maritime Services (IMS) Group

The objectives of the IMS Group are to: enhance and promote EU, regional, national and local cooperation through the exchange of operational best practices; develop an interoperable data exchange platform combining information from SSN and other information systems, and; manage the technical and operational issues related to the IMS functionalities (as defined in Chapter 2.4.2.).

The IMS Group representatives of Member States are nominated by the Point of Contact (PoC). Representatives from other organisations and industry may participate as observers upon pre-approval of the IMS Group as defined in its rules of procedure.

The IMS Group adopts its own rules of procedure, and these constitute part of the SSN technical and operational documentation (as defined in Chapter 1.7).

The IMS Group aims to:

a) define user requirements, map the related business rules and support its adaptation to user requirements;

b) regularly report to MSs, European Commission (COM) and the HLSG on IMS activities;

c) enhance and promote the EU, regional, national and local cooperation through the exchange of operational best practices and experiences.

The IMS Group is responsible for defining the common IMS functionalities, as described in Chapter 2.4.2, as well as specific tools and data, including:

- Integration of the electronic messages and data;
- AIS data collected by satellite (S-AIS);
- Data from other information systems, as defined in the Annex III of the Directive.

The IMS Group is informed about specific IMS functionalities as defined in chapter 2.4.2. When relevant, in order to further support the development of specific IMS functionalities, ad hoc working groups, working manly by correspondence, can be set up by the IMS Group.

EMSA chairs and is responsible for: managing the IMS Group; documenting the above mentioned IMS functionalities, business rules, and related access rights. The IMS Group consults and reports to the HLSG on issues related to the HLSG mandate, as defined in section Chapter 1.4 under "HLSG", or in accordance with the VTMIS Directive (2002/59/EC).

The figure below introduces the user groups and associated groups:

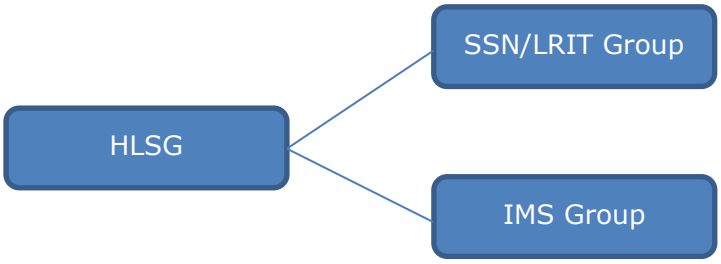

Figure 1 – SSN LRIT and IMS User Groups referenced in the IFCD

1.7 SSN Technical and Operational Documentation

Together with the IFCD, the SSN technical and operational documentation is the reference for the implementation and operation of the national and central SSN systems.

The SSN technical and operational documentation specifies the standards, functionalities and operational guidance that are needed for the system to interact with public and private systems, including the interfaces for automatic transmission of data by electronic means to the SSN. Therefore, for the MSs to comply with the legal framework, the MSs shall follow these documents when setting up a national system.

These documents are developed and maintained by EMSA in cooperation with the SSN group. EMSA is responsible for keeping the latest version of each document updated and available in electronic format on the EMSA website. In order to maintain consistency within and between technical and operational documentation, EMSA and MSs may propose document amendments to the SSN group for approval.

In case of any dispute regarding the interpretation of the documents the IFCD will prevail over the SSN technical and operational documentation.

In addition, the SSN technical and operational documentation contain a part referring to the provision of IMS to Member States.

For LRIT, the technical and operational documentation is defined and maintained by IMO.

1.8 Entry into Force

This document and any revisions to it shall enter into force 20 days after their approval by the HLSG, unless otherwise stated in the text.

Chapter 2 - SafeSeaNet Overview

2.1 Introduction

SafeSeaNet is a system for the exchange of vessel and voyage related information between designated participants within EU. This chapter provides a system overview, discusses the objectives behind SSN and outlines the main flows of information and system functionalities and actors.

2.2 Objectives

The objective of the SSN system is to support EU and MS activities and enable the receipt, storage, retrieval and exchange of information for the purpose of maritime safety, port and maritime security, marine environment protection and the efficiency of maritime traffic and maritime transport.

The operation of SSN involves a number of entities or users at regional, national and local level. The majority of these are in the shipping industry (ships' masters, agents and operators) and national administrations (port authorities and coastal stations, port State control officers, search and rescue (SAR) centres, vessel traffic services (VTSs), ship reporting systems, pollution response bodies, etc.).

By enabling the exchange of vessel and voyage related information, the SSN system supports users at EU and MS level in:

- the **efficient and timely response to incidents or pollution at sea in progress** including search and rescue operations;
- the **monitoring of ships that pose a potential risk to the safety of shipping and the environment**, including those involved in incidents, thus allowing for earlier precautionary actions and risk mitigation at sea by **coastal states**;
- the **effective collection of information in support of the PSC inspection regime**;
- the **effective collection of the required information** on port calls, the carriage of dangerous and polluting goods, security and waste for ships calling into a port of a Member State;
- the **management of flag State responsibilities,** including the follow up of ships involved in incidents/accidents;
- the **efficiency of port calls**;
- the **facilitation of maritime transport**; and
- the **gathering and comparison of objective and reliable information on maritime safety and on pollution by ships,** thus enabling users to take the necessary steps to improve maritime safety and the prevention of ship-generated pollution, and to evaluate the effectiveness of existing measures.

SSN is a specialised system established: to enable the exchange of information in an electronic format between MSs; to provide the Commission with the relevant information in accordance with Community legislation and; to support MSs in satisfying their operational information needs.

SSN is a network of national systems in Member States which are linked to a central SSN system that acts as a nodal point. The central SSN system has different interfaces available to facilitate different means of transmission (see Chapter 2.5.2).

The Central SSN shall allow the sharing, exchange and integration of electronic messages and data, including AIS data collected by satellite, and other relevant data as defined in the Annex III of the Directive in order to provide Integrated Maritime Services. This shall also cover the interfaces with other information systems.

2.3 Mandatory System Functionalities

SafeSeaNet, at the national and central levels, is built upon mandatory system functionalities which are crucial to the normal operation of the system. The mandatory SSN system functionalities are the sending, receipt, storage, retrieval and exchange of information by electronic means required by the SSN legal framework. SSN supports the exchange of the following information:

- **Port call information:** Pre-arrival information sent to ports 24 hours in advance and information on ship arrivals and departures (as per Article 4 of Directive 2002/59/EC as amended and Articles 9 and 24 of Directive 2009/16/EC). In addition, 72 hours pre-arrival information if no other national arrangement is in place.
- **Hazmat information:** Information on the carriage of dangerous and marine polluting goods (as per Articles 4, 13 and 14 of Directive 2002/59/EC as amended).
- **Bunkers information:** Information on the bunkers carried on board a ship leaving or bound for an EU port (reported separately from the notification of dangerous or polluting goods). This notification is to be made available via SSN by Member States that require that information on bunkers on board is reported in their National Single Window.
- **Incident information:** Information on accidents and incidents which have occurred at sea (as per Articles 16, 17 and 25 of Directive 2002/59/EC as amended) and information on ships which have not delivered their ship-generated waste and cargo residues (as per Articles 7 and 12 of Directive (EU) 2019/883) or other information that Member States may consider posing a potential hazard to shipping or a threat to maritime safety, the safety of individuals or the environment.
- **Position information:** AIS, MRS and *LRIT* information (as per Articles 5, 6.b, 9 and 23 of Directive 2002/59/EC as amended).

- **Security information:** Prior to ship's entry into a port of a Member State, security information should be sent in accordance with Article 6 of Regulation (EC) 725/2004.
- **Advance Waste notification information:** Prior to ship's entry into a port of a Member State, the waste including residues information should be sent in accordance with Article 6 of Directive (EU) 2019/883.
- **Waste delivery receipt information:** Before departure or as soon as the waste delivery receipt has been received, the information should be sent in accordance with Article 7 of Directive (EU) 2019/883.
- **Information on persons sailing on board passenger ships:** Before departing, information from passenger ships operating to or from ports of the Member States should be sent in accordance with Articles 4(2) and 5(2) of Council Directive 98/41/EC, as amended.
- **Information on exemptions on ships/scheduled services from the reporting obligations:** on Port call (pre-arrival 24 hours as per Article 4 of Directive 2002/59/EC) and Hazmat (as per Article 15 of Directive 2002/59/EC), Security (as per Article 7 of Regulation (EC) 725/2004), Waste (as per Article 9 of Directive (EU) 2019/883) and persons on board (as per Article 9(2) and derogations as per Article 9(4) of Directive 98/41/EC).
- **Information on exemptions on ports:** Small non-commercial ports in accordance with article 5(5) of Directive (EU) 2019/883 and small ports with unmanned facilities or that are remotely located in accordance with article 7(2) of Directive (EU) 2019/883.

The information collected and exchanged through SSN must comply with the quality and performance standards defined in this IFCD and in the relevant technical and operational documentation.

Administration of user management and locations' codes (LOCODES) are also mandatory system functionalities. Their access rights are defined in the matrix in Chapter 3.4.

2.4 Additional system functionalities

2.4.1 SSN general additional functionalities

SSN provides a number of additional functionalities which are not mandatory and should they become unavailable, it would not affect the operation of the SSN system.

The additional system functionalities are related but not limited to:

- statistics;
- email warnings for giving an indication that there is Incident Report information available in SSN;
- background information display (e.g. nautical charts);
- traffic density mapping products (e.g. traffic density maps, statistics);

- system monitoring tools, and;
- secondary or reference data sources (e.g. SSN users contact details, ship particulars, special lists of ships).

Further functionalities may be incorporated in the SSN system, subject to user demands and approval by the SSN group/HLSG

2.4.2 Integrated Maritime Services (IMS) Functionalities

IMS provide functionalities for the purpose described in Annex III of Directive 2002/59/EC, i.e. maritime safety, marine environment protection, port and maritime security, efficiency of maritime traffic and maritime transport and regional, national and local cooperation for the exchange of additional information.

IMS, through the integration and sharing of relevant data and information, allow the provision of a set of configurable, voluntary functionalities responding to detailed business requirements. IMS integrates SafeSeaNet mandatory and additional system functionalities together with other relevant data from Union information systems, as defined in Annex III point 3 of Directive 2002/59/EC, as amended, as well as Member States or third party specific data sets and information. A non-exhaustive list of information made available via the IMS is:

- SSN mandatory and general additional system functionalities
- Earth Observation (EO) products
- VMS data
- METOCEAN information
- Remote sensing aircraft data

IMS functionalities can be either:

a) **specific**, when they respond to requirements of an individual Member State or group of Member States; or

b) **common**, when they respond to the requirements of all IMS Member States.

IMS are offered to all EU Member States authorities executing functions in the maritime domain.

The common IMS functionalities are agreed by the IMS Group (see Chapter 1.6.2) and referenced in a document named “Integrated Maritime Services functionalities”.

IMS specific functionalities are agreed between EMSA and the Member(s) State(s) requesting for it and the IMS Group is informed accordingly. Should a prioritisation be required for implementing multiple specific functionalities, EMSA, following a dialogue with the involved Member(s) State(s), will introduce the outcomes to the IMS group. The IMS specific functionalities are described in the form of [service] agreements, Service Level Agreements (SLA) or the Operational Level Agreements (OLA) which, inter alia, should

cover: user requirements, the availability, continuity, reliability, access rights, testing, change management and monitoring requirements. The IMS specific functionalities are also referenced in the "Integrated Maritime Services functionalities" document.

The HLSG is informed on the IMS functionalities described above and consulted for approval whenever related to the HLSG mandate, as defined in Chapter 1.4 under "HLSG" and in Chapter 1.6.2 or in accordance with the VTMIS Directive (2002/59/EC).

2.5 SafeSeaNet Architecture

SSN users can access the system via the Internet or the S-TESTA network. In accordance with the Change Management Framework, SSN interfaces are subject to upgrades, amendments and technical improvements. This ensures that the system is updated, correctly implemented and able to cope with the continuous evolution in national, international or EU legislation.

2.5.1 SSN Network organisation

The SSN architecture operates at three main levels:

- National SSN systems.
- The central SSN system.
- External systems for the provision of Integrated Maritime Services.

Figure 2 describes the principles of the Union Maritime Information and Exchange system (SSN) system.

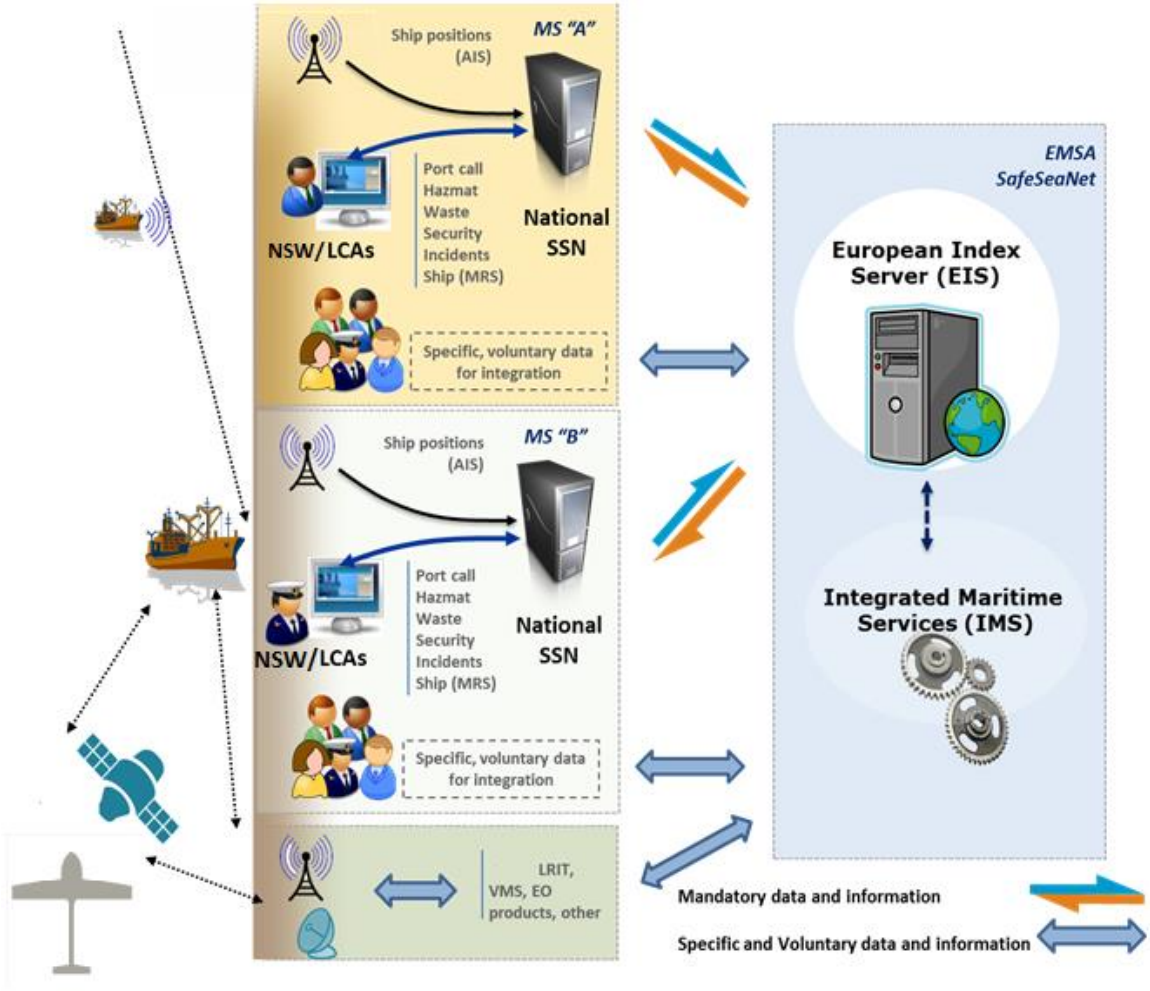

Figure 2 – the Union Maritime Information and Exchange system

LCAs may be data providers as well as data users at local level.

National SSN systems provide information to the central SSN system in the form of notifications. Authorised users within the SSN Community can retrieve information related to these notifications. The central SSN system locates and retrieves this information and provides it to the data user.

While the central SSN system stores some information which enables rapid, effective response to users' requests, detailed information may be stored at national level. When the notifiable information is changed by the data provider, a notification is provided to the central SSN system, and information is updated accordingly.

The NCA may at national level establish a centralised system where all relevant information is registered, stored and exchanged. Alternatively, the details relating to notifications may be stored in the servers of the LCAs.

2.5.2 Information exchange mechanisms

The central SSN system provides different alternative mechanisms to enable the exchange and sharing of data sets and information as described in Chapters: 2.3 and 2.4. These are:

System to System (S2S) mechanisms: These interfaces are available for exchanging data sets and information and perform actions within SafeSeaNet in an automated way using a set of defined formats.

I. **Message-based Interface:** An interface which allows individual messages to be exchanged between: the national and central SSN applications; any other external system and the central SSN, when necessary for the provision of IMS. The messages (e.g. in XML format) fulfil the needs of both data users and data providers (e.g. proprietary protocol, web-services, etc.). The message-based interface supports the notification, request, response and distribution functions for all types of SSN information (Chapter 2.5.3 a).

II. **Geo-spatial Web service Interface:** An interface for discovering, requesting, downloading and displaying geo-spatial information through interoperable and standard interfaces over the web. This interface may be used for the provision of Integrated Maritime Services functionalities as described in Chapter 2.4.2.

III. **Streaming Interface:** An interface which enables the constant flow of data (based on predefined criteria) between: the national systems and the central SSN system (either directly or via an AIS regional server); any other external system and the central SSN, when necessary for the provision of IMS. This mechanism is available for: the provision of AIS information; distribution of the AIS data enriched with information from SSN, or distribution of non-enriched AIS data and; the provision and distribution of integrated vessel position reports or other data related to IMS functionalities. This mechanism is an alternative to the message-based mechanism for AIS data providing (Chapter 2.5.3 b).

IV. **Integrated Reports Distribution (IRD):** The automated or near automated reporting from ships based on information already available in SafeSeaNet ecosystem maximizing potential of the AIS systems and existing information in the central databases (NSW's, SafeSeaNet etc.) and delivering it to authorities via a web user interface, a system-to-system interface and e-mail notifications. The main objective of IRD is to automate the reporting from ships, as much as possible, in order to reduce ships administrative burdens while at the same time improving navigation monitoring by usage of modern technologies and tools.

Central SSN Web browser-based mechanisms: These interfaces are available for requesting information, providing and distributing Incident Reports, displaying and accessing IMS functionalities and may be used to provide other information as a back-up solution in the case of failure of the national or local SSN systems. They are also available for system administration.

V. **Textual interface:** An interface providing direct access to the mandatory functionalities of the central SSN system using a textual layout;

VI. **Graphical User interface:** Single interface using geographical information system technology providing access to: integrated vessel position reports

(including T-AIS, Satellite AIS and LRIT[2]); position reports enriched with the SSN data from the SSN system; satellite remote sensing Earth Observations imagery and derived products; other data and information exchanged or shared in accordance with the relevant Union legislation, and; Member States specific data. This interface provides access to an integrated maritime picture.

VII. **Apps for mobile devices:** This interface provides access to a configurable set of Integrated Maritime Services functionalities via mobile devices (e.g. tablets, smartphones).

For notification purposes, the message-based mechanism and the streaming mechanism are alternative ways of providing Ship AIS positions. The availability and performance standards described hereafter will be applied to the communication mechanism that each MS decides to use in order to fulfil SSN legal framework obligations.

Member States can select the mechanism which best fits their national organisation and technical framework, in order to effectively participate in the SSN Community.

The table below lists the mechanisms available for exchanging information via the central SSN system.

SSN Mechanisms for information exchange		Message-Based	Geo-spatial Web service	Streaming	Integrated Reports Distribution (IRD)	Web Browser-Based		
						Textual interface	Graphical interface	Apps for mobile devices
Available for:	**Data Providing**	All information*	Geo-referenced information	AIS data	Configurable set of data	Incident, exemptions information and In case of failure as a backup mechanism for 72 hours pre-arrival, ATA and ATD	Configurable set of data	Configurable set of data
	Data Request	All information*	Geo-referenced information			All information as per Chapter 2.3	All information*	Configurable set of data
	Data Distribution	Incident reports	Geo-referenced information	1) AIS data enriched with SSN information 2) Ships AIS data	Configurable set of data	Incident reports	Configurable set of data	Configurable set of data

Table 1 – SSN mechanisms for information exchange

* all information related to the Mandatory System Functionalities, as per Chapter 2.3, and a configurable set of information for the additional system functionalities, as per Chapter 2.4

[2] Access to LRIT information is subject to the authorisation of the LRIT National Competent Authority of the MS for their own flag ships

Information will be available via all mechanisms for request purposes, regardless of the mechanism used by the national SSN system when providing information.

Integrated Maritime Services (IMS) may be provided using all the existing mechanisms described above, or via new mechanisms depending on the requirements of the specific users and EMSA resources.

2.5.3 Messaging process

This section covers the provision of the mandatory system functionalities as described in Chapter 2.3.

a) Message based mechanism:

- Notification
  - The *data provider* gathers the necessary information to be reported.
  - This information is sent to the national SSN system or Single Window.
  - The national SSN system compiles the message in the SSN compliant format and forwards it to the central SSN.
  - On receipt the central SSN determines whether the notification is well formed:
    - If well formed, the notification is indexed in the server.
    - If not well formed, the notification is rejected by the central SSN system and the national SSN system should resend the corrected message.
- Request and response
  - The *data user* requests information from the national SSN system.
  - When the information cannot be provided nationally, the national SSN system forwards the request to the central SSN system.
  - The central SSN system verifies the access rights of the user, and subject to acceptance, proceeds as follows:
    - In the case of information stored at central SSN level, the information is sent back to the requester (via national SSN system).
    - In the case of information is available in MS national servers through document download, the central SSN system retrieves directly the document and forwards it to the requester (via the national SSN system).
    - In the case of information is available upon request only, the central SSN system forwards the request to the national SSN system where the information is located, which, may, in turn, forward it to the data provider that owns the information. The data provider that owns the information then responds with detailed information which is transmitted (via the national SSN system) back to the central SSN system for forwarding to the data user.

A sequence diagram describing the above mechanisms is provided in Figure 3.

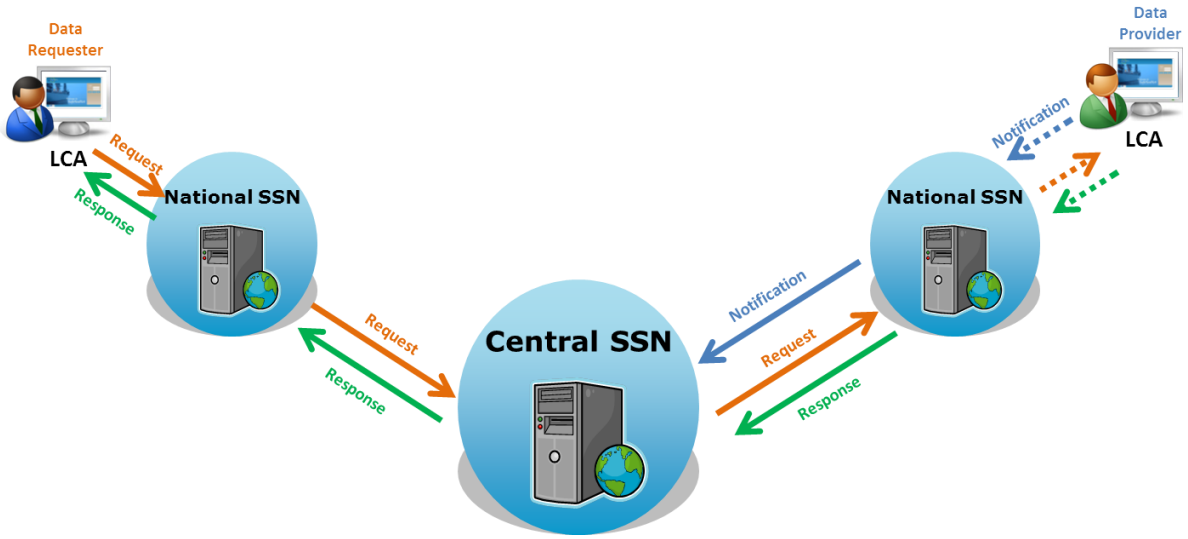

Figure 3 - Sequence diagram of notification, request and response mechanisms

- Distribution for Incident Reports
  - The *data provider* can define the list of recipients for distributing Incident Reports via the national SSN system (in XML) or via the central SSN web interface.
  - The central SSN system verifies the access rights of the user and distributes the Incident Reports in accordance with the distribution list.
  - Incident Reports can be distributed via XML, emails or both depending on the user configuration as follows;
    - If the user is an XML recipient, the central SSN forwards the full information to the national SSN system;
    - If the user is an email recipient, the central SSN distributes emails including basic information about the incident. The full details can be retrieved by the user through the central SSN web interface.
  - The central SSN logs the distribution status and activates a failure management procedure in case of a failure in the distribution.

b) Streaming mechanism:

- Provision of AIS data
  - SSN is equipped with a streaming mechanism which enables the near-real-time exchange of ship positions obtained via the AIS network. This exists at the regional and national levels in order to enable national SSN systems to provide AIS information to regional servers and/or the central SSN system.
- Distribution of Ship AIS data enriched with SSN information.
  - The streaming mechanism supports the distribution of AIS data enriched with SSN information in accordance with the access rights of the user. The data to be streamed is limited to the recipients' corresponding AIS regional server data, or as agreed by the HLSG upon request.
- Distribution of not-enriched AIS data.
  - The streaming mechanism supports the distributing of ship AIS data in accordance with the access rights of the user. The data to be streamed is limited

to the recipients' corresponding AIS regional server data, or as agreed by the HLSG upon request.

2.6 Cooperation with other EU Systems

In this section, the EU systems that interface with the central SSN system at the present time are described, as well as the information exchanged between these systems. A short description of each system is presented below:

- **THETIS** – The Port State Control (PSC) information system developed for the implementation of PSC Directive 2009/16/EC, as well as the New Inspection Regime applicable to the Paris MoU. The system is essential to the daily PSC activities of states operating under the Paris MoU. The entire process (port call registration, targeting, selection, reporting of inspections with corrective actions, publication of details and production of statistics), as stipulated in Directive 2009/16/EC and its implementing regulations, is facilitated by the system.

- **THETIS-EU -** EMSA extended THETIS by developing a new dedicated module (originally named THETIS –S and currently known as THETIS-EU) where users depending on their access rights are able to record and exchange data on inspections and verifications foreseen by EU legislation and not covered by the PSC Directive, while the system facilitates targeting and alerts on the basis of predefined requirements set by EU legislation. Since 1st of January 2015 THETIS EU serves as a platform to record and exchange information on the results of individual compliance verifications performed by Member States as foreseen by Directive (EU) 2016/802 on the reduction in the sulphur content of marine fuels, and since April 2016 serves as a platform to record and exchange information on the results of inspections foreseen by Directive 2000/59/EC (repealed by Directive (EU) 2019/883) on port reception facilities.

- **Earth Observation Data Centre** – The EODC supports a set of earth observation based services including:

    - **CleanSeaNet (CSN)** – The satellite based monitoring service for marine oil spill monitoring and vessel detection in European waters. Operating under Directive 2005/35/EC on ship sourced pollution, CSN provides a monitoring service to national maritime administrations in EU coastal Member States, EFTA countries and candidate countries in their area of interest. The main objectives of CSN are: the identification and tracking of oil pollution on the sea surface; the monitoring of accidental and deliberate pollution and; contributing to the identification of polluters.

    - **Copernicus Maritime Surveillance Service** – This service provides satellite images to support a better understanding and improved monitoring of human activities at sea. The service is available to support a wide range of operational functions, including maritime safety and security, fisheries control, customs, law enforcement, and marine environment monitoring.

EMSA has been appointed as Entrusted Entity of the Copernicus Maritime Surveillance Service, responsible on behalf of the Commission for implementing all technical and operational activities for the duration of the signed Delegation Agreement (2015-2020). The service is provided by EMSA to authorised national administrations in Member States having a function in the maritime domain following a dedicated request.

- **EU Long-Range Identification and Tracking Cooperative Data Centre (EU LRIT CDC)** – Following the adoption of amendments to the International Convention for the Safety of Life at Sea (SOLAS Chapter V), which introduced the long-range identification and tracking of ships, the Council of the EU (in its Resolution of 2 October 2007 and 9 December 2008) agreed to the establishment of a European LRIT Data Centre managed by the Commission through EMSA. Subject to the provisions in SOLAS Chapter V/19.1, Contracting Governments are able to receive LRIT information for security, safety and marine environment protection purposes. Search and rescue services are also entitled to receive, free of charge, LRIT information in relation to the search for, and rescue of, persons in distress. Within Directive 2002/59/EC as amended, the Council agreed to make use of SSN to facilitate the sharing of LRIT information between MSs. The EU LRIT CDC has been in operation since 4 June 2009.

- **LRIT EU Ship Database** – The EU LRIT Ship Database (EU LRIT Ship DB) is a component of the EU LRIT CDC. The purpose of the database is to allow for the registration of ships which have been instructed by their national administrations to report to the EU LRIT CDC. It is accessible online by administrations which are responsible for registering ships, and for updating the identification details as requested by SOLAS Chapter V/19.1. An updated version of the EU LRIT Ship DB is automatically sent on a daily basis to the EU LRIT CDC.

- **Common Emergency Communication and Information System (CECIS)** – The system aims to facilitate communication between the European Emergency Response Centre and National Authorities responsible for Civil Protection and Marine Pollution. CECIS legal background lies in Article 6 of the Council Decision 2007/779 and Article 14 of the Decision 1313/2013/EU. CECIS is a centralised system coordinated by the Commission (DG ECHO). In the field of marine pollution, there is an obligation to report to CECIS requests, or potential requests, for (international) assistance (e.g. requests for EMSA Pollution Response Vessels). CECIS facilitates the exchange between stakeholders by providing a tool for managing requests and offers.

Other relevant EU, national or external systems including

  - **Vessel Monitoring System** (VMS): the system is defined in chapter 1.4. The data owners are the flag Member States.
  - **EUROSUR:** The European Border Surveillance System managed by the European Border and Coast guard Agency (FRONTEX)

- **METOCEAN** providers: the data may be provided via the following services: Copernicus Marine environment, Copernicus Atmospheric service, EMODNET, EUMETSAT, etc.) which define the access rights to apply.

Information exchanged between the central SSN system and other EU systems must respect the access rights policy defined in Chapter 3.
The cooperation between the central SSN system and the other EU systems described above can be summarised as follows. Figure 4 illustrates the process for information exchange between the systems.

- **SSN/THETIS and THETIS-EU:** The central SSN system provides to the THETIS/THETIS-EU system information received from national SSN systems on the port call (pre-arrival 24 hours, arrival, and departure), waste and security information for ships calling at EU ports and anchorages. Within the Integrated Maritime Services, THETIS/THETIS-EU may provide an agreed set of data to the central SSN system.
- **SSN/EODC:**
  The central SSN system provides ship positions and identifiers (transmitted by national AIS networks) to the EODC in order to assist in the identification of vessels and possible polluters for the CSN service.

  The CSN and Copernicus Maritime Surveillance services provide relevant satellite remote sensing Earth Observation imagery and derived products to the Central SSN system for the benefit of the Integrated Maritime Services.
- **SSN/EU LRIT CDC:** The EU LRIT CDC provides LRIT data to the central SSN system. This information is made available to authorised users based on the agreed access rights.
- **SSN/EU LRIT Ship Database:** The EU LRIT ship database provides the central SSN system with ship information in order to validate the ship information held in the SSN system.
- **SSN/CECIS:** The central SSN system provides incident reports of type POLWARN and POLINF to CECIS.
- **SSN/Other systems:** The Central SSN system may be connected to other system(s) for exchanging and sharing data and information in accordance with, and in support of, relevant Union or national legislation. For example:

  - SSN/VMS: the VMS data can be used in IMS for MS for search and rescue purposes.

  - EUROSUR: SSN system provides T-AIS and LRIT, and further transmits S-AIS and VMS data, to EUROSUR

  - METOCEAN data providers provide this information to the central system

Figure 4 – Interfaces of the central SSN system with other EU systems

Chapter 3 - Roles and Responsibilities

3.1 General provisions

As defined in the Annex 3, point 2.1.2 of the Directive, the EU Commission is responsible for the management and development at policy level of the central SSN system and for the oversight of the SSN system in cooperation with Member States. EMSA in cooperation with the Member States and the Commission is responsible for the technical implementation and documentation of SSN and the development, operation and integration of electronic messages and data. EMSA is also responsible for the maintenance of the interface with the Central SSN (including S-AIS, and the different information systems as referred to in Annex III of the Directive, point 3).

With respect to access rights, NCAs and EMSA shall comply with the requirements of the SSN legal framework when managing access to the system.

Access rights should support the performance of the objectives and functions identified in the legal framework or necessary for the operation and administration of the SSN system.

The "competent authorities" (otherwise known as "SSN authorities") designated to perform the above functions or "roles" should have the appropriate access to perform their responsibilities within the SSN system in accordance with the SSN legal framework.

Within each SSN authority, individual persons, persons with the same function and position or systems may be identified as SSN users.

Hereunder are defined: the general rules for user management; the roles for SSN authorities and users, and access rights that should be respected in the implementation and operation of the SSN system. These access rights are applied by EMSA at central level as well as by Member States at national level (within the maximum boundaries).

While Integrated Maritime Services (IMS) promote and facilitate the sharing of relevant data sets and information, the access rights for data other than the ones mentioned in Chapter 2.3 (Mandatory System Functionalities), are set by the data owner and will be followed by the Central SSN system administrator (EMSA) using the exchange mechanisms introduced in chapter 2.5.2.

3.2 User management

The NCA within each Member State is responsible for identifying its own SSN authorities and users at national or local level, and for assigning their roles and access rights.

With the support of EMSA, the Commission is responsible for the management of the roles and access rights for the following types of SSN authorities and their users:

- EMSA and the European Commission for SSN administration and management at central level, including the provision of the Integrated Maritime Services (IMS).
- NCAs for SSN administration and management at national level.

- PoC for IMS for the IMS administration and management at national level.
- Other types of authorities and users, within the conditions decided by the SSN HLSG (e.g. access to other EU Institutions and bodies).

The Central and National SSN administrators are entitled to assign access rights within the boundaries defined per role (see Chapter 3.3.2) for the data referred in Chapter 2.3 (Mandatory System Functionalities).

The Central SSN administrator and the National IMS administrator are entitled to assign access rights within the boundaries defined by the data owner for the Integrated Maritime Services (see Chapter 3.3.2) i.e. data other than the one mentioned in Chapter 2.3 (Mandatory System Functionalities).

They have the right to manage their own SSN authorities and users through a web based application within the central SSN system ("the web management console"). The user management process includes adding, editing and removing users, as well as setting their roles which will define the access rights.

SSN users only have access to the information they have been authorised to use in accordance with the roles and access rights assigned by the SSN administrators at national or EU levels and by the Central SSN administrator or the National IMS administrator for the Integrated Maritime Services.

Access to the SSN system is controlled via a formal user registration process. Each user is identified in SSN by a unique user ID, so that they can be monitored and held accountable for their actions.

The management of users within national applications is the responsibility of NCAs, but the methods used should reflect the principles of the central SSN system.

3.3 Definition of roles

3.3.1 Roles for the Mandatory System Functionalities

SSN administrators assign to SSN authorities one or more of the following functional roles within the system. Each role relates to certain specific SSN system responsibilities in accordance with the SSN legal framework (see Chapter 3.4). The assigned roles should correspond to effective operational functions within the organisation concerned. The provision of the mandatory system functionalities follows a functional approach, i.e. they are independent of the MS governmental department/authority in which users are based. Any user (or set of users) who has (have) been allocated responsibilities which require and justify the use of particular maritime data sets and services, will have access to this data respecting access rights set by the existing legal acts.
The possible roles are:

- **National Competent Authority role (NCA):** for the competent authority or body designated by a Member State at national level as data provider and/or data user (as per the SSN legal framework).

The National Competent Authority Administrator (NCA ADMIN), in addition to the NCA role, has the management responsibility for the national SSN system at national and local level. This role is specific for the national SSN administration and therefore is not reflected in Table 2 below.

- **National Single Window Authority role (NSW):** the competent authority designated by a Member State to implement the provisions of Directive 2010/65/EU, in particular, with the responsibility for overseeing the setting up and operation of the NSW as envisaged for the purposes of this Directive.
- **EU Member States' authorities executing functions in the maritime domain**
  - **Coastal Station role (CST):** with the responsibilities identified by NCAs as data providers and/or data users for vessel traffic services, shore-based installations, bodies responsible for search and rescue and/or pollution response centres (as per the SSN legal framework).
  - **Port State Control role (PSC):** Fulfilling the SSN-related responsibilities of the maritime authority in charge of port State control (in accordance with Directive 2009/16/EC).
  - **Waste Authority role (WASTE):** The "authorities or body designated for this purpose by the Member State" under Directive (EU)2019/883. Their areas of responsibility might be of national scope or limited to one or several ports.
  - **Security Authority role (SECURITY):** the "Competent Authority for maritime security", as defined in Article 2.7 of Regulation (EC) No 725/2004. Its area of responsibility might be of national scope or limited to one or several ports.
  - **Other Users role within Directive 2002/59/EC (VTMIS OTHER):** Fulfilling any other responsibility assigned to a Competent Authority or Local Competent Authority (LCA) in accordance with Directive 2002/59/EC and not covered by the above roles (e.g. Customs, Border guards, Defence or any other legitimate user etc...)
- **Port Authority role (POR):** for the competent authority or body designated by NCAs to receive and pass information to SSN for each port (in accordance with the SSN legal framework).
- **European Commission EMSA or other EU bodies role (EMSA_EC):** EU Commission and EMSA users with responsibilities at EU level.
- **The Central SSN Administrator role (SSN_ADMIN):** SSN_ADMIN fulfils SSN administrator responsibilities at EU level. This role is specific for the general administration of the central SSN system and therefore not defined in Table 2 below.

Central, National and local systems may have their own sets of roles relating to system functions. These should be constructed to balance the need for access to relevant data with the requirements necessary to maintain confidentiality.

3.3.2 Roles for the Integrated Maritime Services functionalities

Integrated Maritime Services develop and implement national, regional and local cooperation and are offered to all EU Member States authorities executing functions in the

maritime domain. The provision of IMS functionalities follows a functional approach, i.e. they are independent of the MS governmental department/authority in which users are based.

Any user (or set of users) who has (have) been allocated responsibilities which require and justify the use of particular maritime data sets and services, will have access to this data and must respect the access rights set by the existing legal acts or the data owner.

The functionalities offered are tailor-made for the user functions, i.e. users can choose which information or data they want to receive for the maritime activities in the defined area of interest, in line with the existing legal basis and/or the access right set by the data owner. The following roles are specific for IMS coordination and administration and therefore are not reflected in Table 2 below:

- **Point Of Contact (PoC) for Integrated Maritime Services role (IMS /PoC):**) assumes, at national level, responsibility for: coordination of data users and data providers, the access rights coordination with the competent authorities;
- **National IMS Administrator role (National IMS ADMIN):** creates users, assigns access rights and functional roles to the IMS users as defined in Chapter 2.4.2.

3.3.3 Roles for the AIS Regional Server functionalities

AIS Regional Server Administrator role (RS_ADMIN): it fulfils the regional AIS server administrator's responsibilities at the regional level. This role is specific only for the administration of the AIS regional system and therefore not defined in Table 2 below.

3.4 Access rights per role

The **access rights** assigned to each role are defined in the matrix in Table 2, which indicates the access rights assigned to each SSN role for the Mandatory System Functionalities, as per Chapter 2.3. These access rights will always apply at central SSN system level for data requesting.
The **access rights** assigned to each role for the IMS services are covered by the SSN ones as per Table 2 below. The Table also indicates the access rights of IMS users for Mandatory System Functionalities that will apply at central level.

Certain cells in the access rights table include **location/condition restrictions,** which limit the access rights of a specific role to a defined area or condition. There are three levels of restrictions:

- Country – limits the access rights to the country where the LCA user is situated (identified in SSN through LOCODES).
- Port – limits the access rights to the port location of the LCA user (identified in SSN through LOCODES). For example, port authorities may only receive, Hazmat, waste, security detailed information from SSN if the requested information concerns their port or ports under their responsibility (i.e. detailed information on ships leaving, or en route to, their ports).

- SAR – Only in the event of an emergency, or in the aftermath of an accident, the information on persons sailing on board passenger ships is made available upon request to other MS designated authorities via the SSN system.

The restriction level is indicated in square brackets [] in the table below. The mandatory SSN data provided through the Integrated Maritime Services functionalities to the authorized users will follow the SSN access rights as per Table 2. An SSN Authority may have one or several roles.

Access rights regarding data and information shared within IMS but not falling in the scope of mandatory system functionality, VMS, EO images and products are governed by access rights rules in accordance with their specific legal bases or contractual agreements.

The SSN User Configuration manual, which is part of the SSN technical and operational documentation, includes further details on the available profiles and correspondent access rights per role in order to assist the users with administration functions to configure the National and Local users.

By analogy, for the IMS information, an IMS User Configuration Manual is available. *[to be further considered if needed]*

Table 2 –The access rights per role defined in the SSN system (national and central SSN systems)

ACCESS RIGHTS / ROLES		National Competent Authorities (NCA, NSW)	EU Member States' authorities executing functions in the maritime domain	Ports	EMSA, EC or other EU bodies users
Data provision	Port call data	**X** [country]			
	Hazmat	**X**			
	Waste	**X**			
	Security	**X**			
	Bunkers	**X**			
	Persons on board	**X**			
	AIS data	**X**			
	LRIT				**X**
	Incidents/ accidents	**X**	**X**		
	Exemptions	**X**	**X**		
	MRS	**X**	**X**		
Data access	All notifications (e.g. Hazmat, Waste, Security, MRS, Incident, Port call, exemptions)	**X**	**X**	**X**	**X**
	AIS data	**X**	**X**	**X**	**X**

ACCESS RIGHTS / ROLES		National Competent Authorities (NCA, NSW)	EU Member States' authorities executing functions in the maritime domain	Ports	EMSA, EC or other EU bodies users
	LRIT Flag reports for all EU MS agreeing to share[3]	**X**	**X**	**X**	**X**
	Hazmat details[4]	**X**	**X**	**X** [port]	**X**
	Waste details [4]	**X**	**X**	**X** [port]	**X**
	Security details [4]	**X**	**X**	**X** [port]	**X**
	Bunkers details [4]	**X**	**X**	**X** [port]	
	Persons on board		**X** [SAR]		
	Incidents/ accidents details [4]	**X**	**X**	**X**	**X**
	MRS details [4]	**X**	**X**	**X**	**X**
	Exemptions	**X**	**X**	**X**	**X**

[3] Those MS not agreeing to share their LRIT Flag reports will access only their own flag reports. The LRIT National Competent Authority will decide whether he/she gives authorization to access these LRIT Flag reports to all the National users globally, or independently for specific LRIT National authority.

[4] Access subject to SSN NCA authorisation when granting the specific profile defined in User Configuration manual.

ACCESS RIGHTS / ROLES		National Competent Authorities (NCA, NSW)	EU Member States' authorities executing functions in the maritime domain	Ports	EMSA, EC or other EU bodies users
	SSN non mandatory functionalities including access to reference databases (E.g. Central ship, Hazmat, Organisation and location databases)	**X**	**X**	**X**	**X**
	Access to statistic information	**X**	**X**		**X**
Data distribution	AIS positions enriched with SSN data	**X**	**X**	**X**	**X**
	Ship AIS data	**X**	**X**		**X**

3.5 Access by users via other EU systems

Access to SSN information by users of other EU systems that are connected to SSN is granted only for the information relevant to their operation (as defined in their legal mandate and respecting the above mentioned access rights per role). For additional details refer to Chapter 2.6.

3.6 Access for users outside the SSN legal framework on a pilot basis

Access may be requested, either on an ad hoc basis (to satisfy a given need during a given period), or in the form of an agreement (MOU), which allows access to SSN by specific users who are involved in pilot projects, but who are outside the SSN legal framework.

In each case, access will be granted only to information relevant to their mandate. The access rights for each user profile shall be determined by a decision of the HLSG for the specific agreed purpose.

Requests for access should be transmitted by the NCA to EMSA, and should provide a precise description of the access requirements, and of the reasons that the information is needed. EMSA, will examine the request in consultation with the Commission, and if appropriate, it will be approved by the HLSG.

Subject to the paragraph above, access may be granted to users involved in pilot projects under the following conditions:

- for a limited period up to one (1) year with possibility of renewal.
- through the web interface only.
- for a specific agreed purpose.
- for a limited number of individual users.

EMSA is responsible to inform the HLSG and the NCAs on any access rights given to users outside the SSN legal framework.

At the end of the pilot project the HLSG or appropriate Council body will review the conduct of the user. Access can then be granted on an on-going basis subject to the signature of a Memorandum of Understanding (MoU) and annual renewal by the HLSG.

3.7 Access for users from the shipping industry

As defined in the Annex 3, point 3 of the Directive, the Commission and the Member States shall cooperate in order to examine the feasibility and development of functionalities that as far as possible will ensure that the data providers (including masters, owners, agents, operators, shippers and relevant authorities) need to submit information only once, taking due account of the obligations in Directive 2010/65/EU[5] and other relevant Union legislation. Member States shall ensure that the information submitted is available for use in all relevant reporting, notification, information sharing and VTMIS systems.

[5] Repealed by Regulation (EU) 2019/1239 establishing a European Maritime Single Window environment

As such, and considering the developments made within the **Integrated Reports Distribution (IRD)**, which consists of automated or near automated reporting from ships based on information already available in SafeSeaNet ecosystem, some information should be made available for users from the shipping industry in order to reduce ships administrative burdens while at the same time improving navigation monitoring by usage of modern technologies and tools.

For this purpose, a ship user account is required to access the system via the web interface. There are two types of account available for the ships willing to submit data electronically:

i. **Self-registered ship account** – The account is created by self-registration and allows ship to create MRS reports and to have access to its own repository of reports. This type of account does not have any connection to SSN data and does not require approval by a Member State.

ii. **Approved ship account** – to have access to re-use information available from the SafeSeaNet ecosystem, access must be approved by a Member State NCA or by an authority associated to the MRS to which the ship is required to report. Access to SafeSeaNet ecosystem information for their own specific vessel is limited to:

- Voyage related information (port of call, ETA to port of call, number of persons on board (POB));
- Indication of Hazmat on board (yes/no indicator, with possible access to Hazmat details in the future);
- Previous MRS report to SSN;
- AIS data (position coordinates and time stamp, SOG, COG, draught, navigational status, Next Port of Call and ETA).

Note: The use of the IRD service for electronic ship reporting is **optional** and is considered as additional mean of reporting to existing radio communication or e-mail reporting. The use of electronic reporting requires an amendment of the existing Mandatory Ship Reporting system at IMO. For the moment this process has been initiated exclusively for ADRIREP system at the IMO and is expected to be adopted by the MSC 101 in May 2026 with implementation six months after adoption.

3.8 Access by non-SSN participating countries for reporting MRS

For countries that share an MRS with EU Member States and that are willing to modernise their current MRS implementation with the developments made within the **Integrated Reports Distribution (IRD)**, the MRS information reported via SafeSeaNet ecosystem for their specific MRS system shall be made available to non-SSN participating countries.

The reciprocity principle should apply, thus non-SSN participating countries should share their MRS reports with EU Member States via SafeSeaNet ecosystem.

To be noted that non-SSN participating countries will not have access to information which is not already available to them in the SRS.

3.9 Access for other organisations to submit Incident Reports

Access may be granted for other organisations for the specific purpose of submitting Incident Reports, based on the justification of the operational benefit to the SSN community. Access shall be determined by a decision of the HLSG for the specific agreed purpose.

Requests for access should be transmitted to EMSA, and should provide a precise description of the incidents to be reported via SSN and their operational benefit. EMSA, will examine the request in consultation with the Commission, and if appropriate, it will be approved by the HLSG.

Subject to the paragraph above, access may be granted to users from these organisations under the following conditions:

- for a limited period up to one (1) year with possibility of renewal, following assessment by HLSG.
- through the web interface only.
- for a specific agreed purpose.
- for a limited number of individual users.

EMSA is responsible for informing the HLSG and the NCAs regarding any access rights given to users under this paragraph.

Chapter 4 - SafeSeaNet Performance

The following performance requirements apply to the processing of messages and system information.

Member State authorities may assign more specific performance standards in accordance with their national requirements.

4.1 Timeframes for Data Availability

The national SSN systems and the central SSN system (which includes the provision of the Integrated Maritime Services - IMS) should be supported by data communication links and networks that allow them to transfer information between the two systems within 1 minute. This timeframe should be respected for 95% of the information exchange over a 24h period, and for 99% over a one year period.

SSN data users should receive the desired information from SSN within an average of 30 seconds (central SSN system will not process responses received after 4 minutes) of making a request. Member States should aim at an average response time much lower than this maximum to meet the operational needs. In the case of phone, fax or email, they should receive the requested information within 60 minutes. This is not applicable to archived information (see Chapter 4.2).

4.2 Timeframes for Data Storage

The data shall be directly available in the **SSN system** for:

a) a minimum of 5 years for information related to incidents and accidents, and;
b) a minimum of 2 months from the departure of the ship for information related to port calls, hazmat, security, waste and cargo residues; and from the reporting date for ship position information;
c) a minimum of 6 months for the Integrated Maritime Services data stored centrally.

In any case, the data should be **archived** for at least 5 years, down-sampled when necessary. The archived data should be made available when requested by NCAs or EMSA, on the basis that the requester must provide a justification for why the information is required. Among other things, archived data may be used for purposes such as: obtaining historical positions of ships involved in illegal activities; violation of rules; statistical analysis or; studies on traffic flows.

NCAs should respond to requests for archived data within 5 working days. The exchange of archived data is done through alternative communication means (see as per Chapter 4.7).

4.3 System Availability Requirements

This section refers to the availability of the hardware and software necessary for the provision of the mandatory functionalities of the SSN system (see Chapter 2 - SafeSeaNet Overview).

SSN shall be maintained in operation twenty-four hours a day, seven days a week, to satisfy the mandatory system functionalities of the SSN system.

The availability of the SSN system shall be maintained at a minimum of 99% over a period of one year, with the maximum permissible period of interruption being 12 hours.

The availability requirements above apply independently to each national SSN system (including the communication links to the central SSN and local systems) and to the central SSN system (and communication links to the national SSN systems).

The availability of the hardware and software components at EMSA, necessary for the provision of the common IMS functionalities (see Chapter 2.4.2) are the same as the ones described for the SSN Mandatory System functionalities.
The requirements for the provision of the specific IMS functionalities (see Chapter 2.4.2) are described in the form of specific [service] agreements, Service Level Agreements (SLA) or Operational Level Agreements (OLA).

4.4 Backup Procedures

Backup procedures should be in place for each SSN system component, and should be implemented in the event of a failure or a scheduled interruption (as described in the SSN Technical and operational documentation).

In the event of a failure or a schedules interruption, NCAs shall ensure that SSN messages are stored and then transmitted to the central SSN system when communications and/or systems have recovered. The national and central SSN systems should be able to re-send messages for up to 2 weeks (ship position information may be down-sampled for this purpose).

The body responsible for the affected SSN system component must inform the other SSN system participants according to the operational procedures whenever a failure or scheduled interruption occurs.

4.5 Additional System Performance Requirements

Invalid messages will be rejected by the central SSN system, and an error message will be sent back to the national SSN system. In cases where the central SSN system transmits an invalid message, the national SSN system should inform the MSS of the reasons for the invalid message as soon as possible.

Invalid messages (those not compliant with the standards set in the SSN Technical and operational documentation) should be less than 0.1% of the total number of messages sent.

All participants should aim to prevent invalid messages from being sent.

4.6 Data Quality

MSs should ensure that the automatic data quality rules agreed by the SSN group are applied prior to notifications being sent to the central SSN system. In case missing or mismatch information has been discovered, this should be corrected as soon as possible. Such an adjustment should be traceable.

Missing information (provided in accordance with chapter 2.3) should be less than 0.1% per type.

In liaison with EMSA, MSs should set in place appropriate control mechanisms to investigate data quality issues that affect more than 0.1% of the reports per country and type (see Chapter 2.3) per month.

4.7 Operational Coordination

Each NCA and EMSA should maintain a 24/7 contact point that is available to manage SSN Mandatory System Functionalities related requests relating to daily operations or reporting issues from any other NCA or EMSA.

The EMSA Maritime Support Services (MSS) provides 24/7 monitoring of notification requirements and network coordination as well as a helpdesk for the SSN system.

The monitoring and operational communication procedures to be used for interaction between the NCA 24/7 contact points, National IMS Administrators and the MSS are agreed at the level of the SSN and IMS groups (when applicable and within the framework of Chapter 5).

Chapter 5 - Operational Services and Procedures

5.1 Overview

This chapter provides a framework for the operational services and procedures to be maintained by both national and central SSN systems to ensure the correct operation of the SSN system including the Integrated Maritime Services (IMS).

For this chapter operational services and procedures are understood as services and procedures that require human intervention.

MSs and EMSA should take necessary steps to ensure that operators of the national and central SSN systems are appropriately trained to perform their duties.

5.2 Operational Services

5.2.1 System Support Services at National Level

Member States shall ensure that effective exchange of the information referred to in the SSN legal framework takes place at national level.

This information exchange may be executed by means of the designated **24/7 NCA** services, which could include the following elements (on a 24/7 basis):

- Respond to direct requests for information from a SSN user by phone, fax or e-mail: MSs are obliged to respond to SSN requests in accordance with the agreed response times mentioned in Chapter 4.1.
- Respond to requests for information from a MS NCA 24/7 or MSS by phone, fax or e-mail, during a Business Continuity event (in accordance with Chapter 5.2.4).
- Provide an SSN Incident Report distribution service at national level: Incident Reports received from another MS via SSN should be distributed among the relevant LCAs within the country.
- Monitor the performance of the communication system within its service area in order to assess any degradation in its operational capability.
- Monitor data providers' communication links.
- Monitor the NCA's own operations in order to ensure availability and to avoid the distribution of unreliable or corrupted messages.
- Immediately notify the MSS should the national system be unavailable to receive, process or transmit data in accordance with the IFCD specifications.
- Receive information on reported technical failures from the MSS and distribute to national users whenever required (e.g. failures in another MS or in the SSN application/hardware/network).
- Provide support to users at national level.

The NCA should also ensure that additional SSN related services, such as the following, are carried out (not on a 24/7 basis):

- Managing reference databases at national level (see chapter 5.2.3).
- Administrating users' access at national level.
- System assessment relating to the quality of the information provided by the national SSN system.
- Providing feedback to the SSN development teams.
- Providing archived data following requests from NCAs or EMSA.
- Ensure that the company, who has been given an exemption in accordance with Article 15 of the Directive 2002/59/EC as amended, has established an internal system that makes it possible for the NCA to receive the due information.
- Designation of the list of competent bodies according to Article 20.a.3 and Article 22 of Directive 2002/59/EC.
- Ensure that the information is reported to the central SSN system on granted exemptions regarding:
    - Pre-Arrival 24 hours and Hazmat (in accordance with Article 15 of the Directive 2002/59/EC as amended)
    - Security (in accordance with Article 7 of Regulation (EC) 725/2004)
    - Waste (in accordance with Article 9 of Directive (EU) 2019/883)
    - Persons on board (as per Article 9(2) and derogations as per Article 9(4) of Directive 98/41/EC)

Integration, exchange and sharing of data within the Integrated Maritime Services (IMS) are voluntary processes and, for relevant data sets, may be subject to separate agreements (SA, SLAs or OLAs), per service, between EMSA, data providers and/or the end-users (Member States).

5.2.2 Central System Support Services

In accordance with the definition provided in Chapter 1, EMSA is responsible, on behalf of the European Commission, for the management of the central SSN system. This includes: monitoring the continuity of service at the centre; connections with Member States; monitoring and reporting on data quality and availability; IT and engineering support restricted to the user interfaces and; communication interfaces within SafeSeaNet.

EMSA provides these services via its 24/7 **Maritime Support Services (MSS)** operations centre. The services provided on a 24/7 basis are as follows:

- Monitoring the availability and performance of the central SSN system, including the Integrated Maritime Services functionalities.
- Support Member States in the monitoring of the national SSN systems in terms of availability and data quality of the information exchanged (i.e. the availability of

notifications, rejected messages, details in ship positions, Hazmat and incident information).

- Provision of an operational and IT helpdesk for central SSN users (e.g. NCAs) including IMS users.

The MSS also provides the following SSN support services:

- Management and validation of the reference databases in the central system.
- Administration of user accounts within the central system, and in particular, managing the list of NCA contacts to be used for communication purposes.
- Provision of statistics on SSN activity by Member State and type of message.
- Testing of new versions and provision of feedback to development teams.

5.2.3 Reference Database Management

Reference databases are those used at the central, national and local levels to support reporting obligations. A non–exhaustive list of the potential databases includes: the location codes database (LOCODES), the central ship database, the users database and the dangerous and polluting goods database.

Data exchanged within the SSN system (including IMS) should be coherent and of the best possible quality. Therefore, where practical, the reference databases should be the same for all NCAs and POC's for IMS and their systems. These may be developed and managed centrally by EMSA in order to harmonise the data and to avoid inconsistencies that may occur as a result of using too many different databases. These central databases should be agreed by the relevant SSN user group(s), and should be made available to all users to improve the quality of the information in the system.

5.2.4 Continuity of Service

To cover unforeseen crises, disasters and/or general disruptions to normal system operations, business continuity measures should be in place in order to ensure continuity of service at both the national and central levels. These should be able to guarantee that: the SSN system remains able to perform its mandatory functionalities (listed in Chapter 2.3) and the Integrated Maritime Services functionalities (as described in Chapter 2.4.2); to the fullest extent possible. These measures are separate from those required to meet the performance standards in sections 4.1 and 4.3 under 'normal' conditions.

The business continuity measures should be defined at national and central level and aim at:

- Ensuring, by means of the alternative solutions, that the mandatory information required by the SSN legal framework can still be available on request, and;
- Ensuring that information is recoverable to the fullest extent possible after a down-time period/disaster/failure.

5.3 Operational Procedures

Operational procedures should be defined at both the national and central levels in order to support the operational services defined in Chapter 5.2. These procedures should be described and documented in local manuals and/or in the SSN technical and operational documentation.

The operational procedures should be available to all system support services staff in electronic and/or printed form, and they should be an integral part of regular training activities.

Updating the procedures should be a continuous process, and NCAs should ensure that updates are also made available to all systems support services staff. This should ensure that they are made aware of all relevant changes, and that new procedures are understood and properly implemented.

Operational procedures which only affect national SSN systems should be defined at national level and are not covered by the IFCD.

The main non-exhaustive list of general operational procedures which affect the different types of SSN users in different MSs is as follows:

a. **Reporting technical failures or planned interventions**
   The purpose of this procedure is to ensure that data providers and users receive appropriate information on technical failures or planned interventions in the SSN system.

b. **Providing information during system failures or planned interventions**
   The purpose of this procedure is to ensure that, during short periods of system failure or planned interventions, MSs are still able to request information stored at national level using alternative communication means. This back-up procedure only applies to limited requests during maritime emergencies.

c. **Distributing Incident Report notifications to other MSs**
   The purpose of this procedure is to harmonise the process of distributing and storing information on Incident Reports.

d. **Reception of distributed Incident Reports**
   The purpose of this procedure is to ensure the proper information flow for the distribution of incident reports.

e. **LOCODES management**
   The purpose of this procedure is to manage the reference list of LOCODES in the SSN system.

f. **Updating the list of NCA and LCA details**
   The purpose of this procedure is to maintain an updated list of NCA and LCA details, including the NCA 24/7 contact and others related to the management of SSN system. The list should be communicated to the MSS.

g. Missing or mismatched information in SSN

The purpose of this procedure is to investigate and correct any detected inconsistency in the information provided to the SSN system, including ship details (IMO, MMSI, Call sign and name).

h. Requesting and providing historical data

The purpose of this procedure is to harmonise the way that archived data can be requested from any data provider (see Chapter 4.2).

i. Communication procedure

The purpose of this procedure is to establish an identification method for data exchanged between two different MSs using communication means such as phone or email. In such cases, the communication should be re-directed through the NCAs to allow for proper identification (based on the most recently updated SSN contacts list in the system).

j. Exemption procedure

The purpose of this procedure is to harmonise the process for recording information on exemptions through the central SSN system. It also clarifies how to retrieve information on exemptions.

k. Communication of the list of competent bodies

The purpose of this procedure is to establish the process whereby MSs provide and update information on their coastal stations and places of refuges related information to the Commission, as required by Article 20.a.3 and Article 22 of Directive 2002/59/EC.

l. Integrated Maritime Services specific procedure (s)[6]

The purpose of this procedure (these procedures) is to establish and harmonize actions related to the provision of Integrated Maritime Services functionalities as per specific [service] agreements, SLAs or OLAs established between data owners, EMSA and/or end-users. These procedures may cover, among others, the provision of Automated Behaviour Monitoring (ABM), specific and integrated vessel position report data, satellite remote sensing Earth Observation imagery and derived products and, if applicable, other applicable data sets or information.

[6] These procedures, where necessary will be identified separately

Chapter 6 - System Management and Tests

6.1 Change Management Framework

6.1.1 Overview

The SSN group is responsible for the technical and operational management of the SSN system, including the integration of added value functionalities when approved by the HLSG, and also requirements arising from new or revised legislation. The implementation of new requirements at the national and central levels requires close coordination between MSs and EMSA.

The SSN Change Management Framework (CMF) document, which is part of the SSN technical and operational documentation, describes the procedure/process by which changes to the SSN system are decided upon, introduced and managed. This framework applies to all parties in the SSN system, including the participating MSs and EMSA. The objective of the CMF is to:

- establish a formalised and binding Change Management Process (CMP) via which changes to the SSN system are introduced, coordinated and evaluated;
- identify the actors involved in the CMP, along with each actor's roles and responsibilities;
- determine methods for classifying and prioritising change proposals;
- establish documentation and reporting standards in order to provide an appropriate measure of accountability for changes made using the CMP, and;
- manage modifications to the CMP.

Changes to the CMF will be proposed to the SSN group by participating MSs or EMSA.

6.1.2 Change Management Scope

The CMF will be invoked for all proposed changes to SSN system.

The first stage will be the evaluation of the impact of any requested change. Should the evaluation determine that the change request will have an impact on SSN (at the central and/or national levels), further steps in the change management procedure/process will be applied. The decision making process will reflect the type and extent of any impact on the SSN documentation and its specifications:

a) When there is an impact on the IFCD, a decision of the HLSG is needed.

b) Changes affecting mandatory SSN documentation require a decision of the SSN group.

c) In other cases, a decision by EMSA is sufficient, subject to consultation with the SSN group.

The CMF is the framework for managing changes which result from EU directives or legal obligations, but it cannot be used to block such changes or to increase the scope of the set requirements.

6.1.3 Change Management for the Integrated Maritime Services functionalities

The Integrated Maritime Services (IMS) Group is responsible, inter alia, for the technical and operational management of the Integrated Maritime Services, including the change(s) to existing functionalities, and the development of new functionalities, as defined in chapter 1.6.2.

Changes covering only specific Integrated Maritime Services (IMS) functionalities (see chapter 2.4.2 a) shall be described in a standardized form, agreed between EMSA and the relevant stakeholder(s). The Integrated Maritime Services (IMS) Group shall be informed of these changes accordingly.

Changes covering common Integrated Maritime Services (IMS) functionalities (see Chapter 2.4.2 b) shall be described in the standardized form agreed between EMSA and the relevant stakeholder(s). Thereafter these changes shall be validated by the Integrated Maritime Services (IMS) Group.

The IMS group shall consult the HLSG on the changes related to the Integrated Maritime Services functionalities as described in chapters 1.6.2 and 2.4.2.

EMSA is responsible for documenting the changes to IMS business rules, access rights and functionalities.

6.2 System Commissioning

6.2.1 General Guidance

Before connecting with the production site of the central SSN system, an NCA shall perform commissioning tests on the national SSN system and provide the data specified in the "MS Commissioning Test Plan" document, which is part of the SSN technical and operational documentation, to the SSN system manager (EMSA). The commissioning tests verify that the system developed by a MS is able to exchange messages in accordance with the system specification.

The commissioning process is required to ensure that national SSN systems can support the reliable, timely and accurate exchange of data and system information within the overall SSN system. The commissioning process is also required whenever there are major changes to SSN system interfaces.

The commissioning process is defined in the "MS Commissioning Tests Plan" document, and it covers all system functionalities and information exchange mechanisms adopted by national SSN systems.

6.2.2 General Commissioning Procedure

Commissioning tests are performed at the request of MSs, and the results shall be documented in a test report. The test report, and the associated data files (if any), are to be submitted to EMSA for assessment.

EMSA shall analyse and evaluate the test report and, if the test results comply with the SSN requirements, EMSA shall aim to validate the results within 2 weeks. Once the results have been validated, EMSA issues a test acceptance form and updates the status of operation of the MS concerned. Via this process, the MS becomes an officially recognised participant in the SSN network for the designated functionality.

The acceptance is then communicated to the SSN group.

MSs may perform tests for a part, or parts, of the system and gain approval only for the designated parts. In cases where MSs choose this option, they must still undergo tests for the remaining part(s) of the system requirements before they can use them in production.

Chapter 7 - System Security

7.1 General provisions

The following chapter describes the security policy that applies to the processing of messages and system information at central SSN system level.
The baseline security requirements hereunder should be mandatory for the central system and its interface with the National SSN systems and be referred to as optional at national/local level.

Further details about the requirements of this chapter can be found in the SSN Technical and Operational Documentation which includes the SSN security vocabulary.

The SSN authorities may assign higher security measures on the system components they manage due to their specific needs and policies as long as these additional measures do not limit the ability of duly authorised SSN users to access relevant information.

7.2 Security Policy

7.2.1 Organisational Aspects

SSN Authorities implementing the SSN system in form of hardware and software and/or with responsibilities in terms of provision of access rights to the SSN system should clearly assign to specific responsible individuals the following minimum security related functions:

a. Functions related to security management:
   - Evaluation of requests to become a SSN user, against the user management rules in Chapter 3 and any other specific rule on access rights;
   - Association of user roles and sets of user access rights;
   - Ensuring, facilitating and carrying regular system security audits;
   - Carrying out of training courses on security matters;
   - Proposing review and update of the security policy of the authority; and of the security requirements deriving from the IFCD and the SSN documentation to the SSN group.

b. Functions related to security implementation:
   - Technical implementation and monitoring of the security measures deriving from the IFCD and the SSN documentation;
   - Technical implementation and monitoring of the security policy of the authority.

The above functions shall be adjusted to the needs and the organisation of each Member State.

7.2.2 General security measures

7.2.2.1 Access Control

a. SSN Authorities implementing the SSN system in form of hardware and software should keep record of individuals gaining physical access to it.

b. Tailoring of privileges granted to an SSN user by the NCA administrator shall be performed as per access rights policy defined in Chapter 3.

7.2.2.2 Authentication

c. A reliable authentication mechanism shall be implemented to uniquely identify the SSN users.

d. Passwords should be compliant with the SSN password policy detailed in the SSN Technical and Operational Documentation.

e. The creation of User IDs should follow the naming convention defined within the SSN Technical and Operational Documentation.

f. SSN Authorities implementing a web user interface shall guarantee the security of the transmission of information through the web user interface by appropriate means based on industrial best practices. For the central SSN web interface 1-way SSL will be implemented (using certificates issued by a globally trusted CA).

g. SSN authorities implementing a system interface shall guarantee the security of the transmission of information through the system interface by appropriate means based on industrial best practices. For interfaces with the central SSN system 2-way SSL will be implemented (using certificates issued by the EMSA CA).

h. A user ID should only be used by the appointed SSN user or users. Authorities in charge of providing access to the SSN system should keep a record of all accesses per user ID at their system level.

i. A review of the credentials (e.g. password modification, user account revocation) used to access the SSN system should be performed at each system level regularly (at least each year) or whenever there is an upgrade of the SSN security policy affecting the authentication mechanism (e.g. SSN password policy).

7.2.2.3 Authorisation

j. Authorisation of the NCA by EMSA should be subject to the identification of the individuals responsible for the security management and security implementation.

k. SSN Authorities should grant access only to users in accordance with the rules in Chapter 3.

l. A review of the authorisation/access rights) should be performed at each system level at least each year or whenever there is an upgrade of the SSN security policy affecting the authorisation protocol (e.g. change in the access right policy).

7.2.2.4 Non-repudiation

m. Central SSN system allows the verification of the history, location, or application of the information from the mandatory system functionalities (as per chapter 2.3) by means of documented recorded identification. NCAs are responsible for collecting this security data at national level.

n. The following actions shall be traced and the records shall be available to the data provider of the information upon request:

- Receipt of the information.
- Modification of the information.
- Requests for the information.

o. The information recorded shall be as follows:

- User identification[7].
- Time stamp.
- Description of action.

p. Each SSN system (national and central) shall ensure the non-repudiation and traceability of actions performed by SSN users accessing the system by means of both automated systems (message based and streaming mechanism) or the web interface (web-browser based mechanism). An administration providing the information can request the identity of the data requestor, without delaying the response.

7.2.2.5 Data Protection and Confidentiality

q. SSN Authorities implementing the SafeSeaNet system in form of hardware and software and/or with responsibilities in terms of provision of access rights shall ensure that the confidentiality of the data stored within or exchanged by those system components they are responsible for is not compromised. Data protection procedures shall be put in place. The protection procedures for the data exchange are specified in the SSN Technical and Operational Documentation.

r. The SSN system shall manage data according to their confidentiality level for both data exchanged and data stored. According to Commission Decision 2001/844/EC amending its internal Rules of Procedure by annexing Commission Provisions on Security, the SSN system is classified as an "unclassified system".

s. SSN includes some commercial sensitive data, system security related information and personal data as follows:

- "Commercial Sensitive" : information on dangerous and polluting goods, incidents, cargo residues and port call information;
- "System Security related" : user authentication information;
- "Personal data":

[7] In case a user account is shared by a group of people sharing the same functions, the identity of all the persons that make use of the account shall be available.

- users' credentials,
- first names, last names, nationalities, dates of birth and genders of ships' crew,
- first names, last names, nationalities, dates of birth, genders, information concerning special care or assistance and contact numbers of ships' passengers,
- first name, last name and contact details of ships' CSO.

t. Data storage shall be performed in accordance with the following rules:

- System Security Related data shall be stored encrypted;
- Personal data should be stored in accordance with bullets (x) and (y) below and shall be stored encrypted.

u. Users shall not provide information to any unauthorised persons or systems.

v. Users shall not disclose their login credentials to unauthorised persons.

w. Users shall not provide to the SSN system classified information as defined by Commission Decision 2001/844/EC.

x. The principles of personal data protection as defined in Regulation (EU) 2018/1725 shall be applicable to any information concerning an identified or identifiable person exchanged through the Central SSN system.

y. National SSN systems shall comply with Regulation 2016/679 (GDPR) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

7.2.2.6 Integrity

z. SSN shall ensure that the information is authentic and complete. The information transmitted via the central SSN system shall only be modified by:

- the data provider;
- the NCA covering the data provider, or;
- the central SSN system (in accordance with the rules/procedures defined in the SSN documentation).

aa. The management of data provision shall ensure that all reasonable steps have been taken to prevent denial of service attacks, the introduction of 'malware', or other malicious events with the potential of compromising SSN functionalities.

bb. Data Minimization thinking should be applied to log collection. Steps must be taken to ensure integrity of the transmitted data while optimising storage of logs.

cc. The list of hardware and software, used to implement the SSN system or used within the authority to interface with it, should be recorded in a register. This register should be maintained during the whole system lifecycle.

7.2.2.7 Training

dd. Authorities should ensure that all system users within its jurisdiction are aware of the security requirements of the system and have the knowledge and competencies to fully discharge their obligations.

7.2.2.8 Audit

ee. Security audits on the SSN system implementation and usage should be carried out on a regular basis or in case of events defined within the SSN Technical and Operational Documentation. Whenever possible existing audit arrangement will be accepted as the fulfilment of this requirement.

ff. Proactive monitoring should be applied. Security monitoring and investigation should occur NOT ONLY in case of a security breach. Monitoring for unusual or suspicious activity should be performed on a regular basis.

7.2.2.9 Other Security Requirements

gg. At network architecture level, a differentiation must be made between presentation, business logic and data layers, whenever possible, following a three-tier architecture.

hh. SSN systems should ensure user input validation whenever possible, to prevent injection attacks and unauthorised access to data.

ii. SSN systems should proactively mitigate known vulnerabilities, and all its technological components (e.g. operating systems, databases, and application server) should be continuously updated.

jj. A periodic penetration test (Pentest) should be scheduled for SSN systems every time a new version of the application is released or at least every two (2) years, coincidently with the end of the life/support of different technologies that could be implemented in the SSN system.