European Maritime Safety Agency

SafeSeaNet Workshop no 10
Agenda item VI
Lisbon, 24 September 2008

SSN 10/6/1 (v.1.0)
21 & 22 October 2008

ADMINISTRATIVE ISSUES

SSN Handbook

Submitted by EMSA

Executive summary	This document presents the SSN Handbook.
Action to be taken	To agree on the content for the SSN Handbook To disseminate it among the SSN users in MS.
Related documents	SSN 9/6/1

1. INTRODUCTION

This is a follow-up to the proposal presented during SSN WS 9.6.1. Member States are asked to revise the proposal of the SSN Handbook, agree on the content and on the implementation date of the document.

2. THE PURPOSE OF SSN HANDBOOK

The SSN Handbook in annex 1, prepared by EMSA at the request of the MS, aims at linking procedures described in existing SSN documents and presenting them together. The SSN Handbook does not supersede or replace any of those existing SSN documents.

The target readers of the SSN Handbook are:

- Users working at National Competent Authority (NCA) level in the Member States; responsible for local SafeSeaNet implementation, administration and operation as well as Technical Teams (TT) responsible for the development and maintenance of the system;

- Users working at Local Competent Authority (LCA) level in the Member States (Port, PSC, Coastal Stations and others) which gather, send to SSN or store detailed information on ships' movements;

Landlocked Member States (mainly WEB users) and System Administrators (EMSA, Maritime Support Services operators) can also profit from the use of the Handbook.

EMSA intends to maintain the Handbook as a SafeSeaNet "umbrella" document, for use by Member States (translated into each national language) and to keep it up to date as

new technical or operational requirements are adopted. Following that, EMSA will also explore the possibility of drafting a comprehensive manual that can be used by the shipping industry (masters, agents, operators) as a guideline for the minimum SSN requirements.

3. PROPOSED IMPLEMENTATION SCHEDULE

EMSA distributed in September 2008 first draft of the SSN Handbook for revision. Member States provided their comments and feedback. Following that process EMSA is going to send a final revised version by 1st November, in order to incorporate any comments/proposals made during the WS10 and will publish the SSN Handbook on its WEB Page. Any changes regarding the content of the Handbook will be announced on the WEB page and via a general e-mail.

4. ACTIONS PROPOSED

For Member States:

- to agree at SSN 10 on the main lines of the SSN Handbook;
- to revise the final version that will be sent by 1st November by EMSA;
- to disseminate final version of the Handbook among SSN users within each Member State.

For EMSA:

- to send the SSN Handbook to MS for final revision by 1st November;
- to publish the document at SSN website.

European Maritime Safety Agency

SafeSeaNet Handbook

Version 1.00, 12 September 2008

SafeSeaNet guide for the Member States' National and Local Competent Authorities (NCA & LCA)

Table of Contents

1. Introduction 3

1.1 SSN Handbook objective 3
1.2 Users 4
1.3 How to use the Handbook? 4

2. Questions per subject 6

2.1 Contact details and account management 7
2.2 Testing/ Internal training phase and commissioning tests 8
2.3 Digital Certificate 9
2.4 Initial Operation Phase (I.O.P) 10
2.5 Operational Procedures 11
2.6 Management of technical failures and new versions of the SSN 12

3. Control Lists 13

INDEX and format 14
1.0.1 – SafeSeaNet Welcome on Board document update 16
2.0.1 - Commissioning Tests 18
2.0.2 – Commissioning Tests Reporting 22
3.0.1 – Request for the Digital Certificate 23
4.0.1 – Initial Operation Phase (I.O.P) 26
5.0.1 – Request for information 27
5.0.2 - Request for the follow-up action 28
5.0.3 - Update of LOCODES 29
5.0.4 – Alert Messages Guidelines 31
6.0.1 – Technical Failure 32
6.0.2 - Change Management Plan – changes in business logic 33
6.0.3 – New releases, description and announcements 35

Annex 40

Abbreviations and Acronyms 40
References & supporting documentation 41

1. Introduction

1.1 SSN Handbook objective

The main objective of SafeSeaNet is to provide a European platform for maritime data exchange between maritime administrations of the Member States, by setting-up a telematic network between all the maritime EU Member States, Norway and Iceland for their co-operation in preventing maritime pollution and accidents at sea. The SafeSeaNet System is implementing the exchange of information foreseen by European Parliament and Council Directive 2002/59/EC of the 27 June 2002, establishing a Community vessel traffic monitoring and information system.

The core of the SafeSeaNet architecture (EIS) consists of the SafeSeaNet XML Messaging System. It acts as a secure and reliable "yellow pages" index system in a "hub and spoke" network (including authentication, validation, data transformation, logging) for sending requests to and receive notifications and responses from users identified as *Data Providers* and *Data Requesters*.

Detailed factual information is stored at Member State level. Whenever the information changes the Local Competent Authority - LCA (normally via the National Competent Authority - NCA), sends a notification to the EIS and the EIS is up-dated with the location of the information.

SafeSeaNet is continuously evolving. Decisions on technical changes are taken during SSN Workshop meetings co-ordinated by EMSA[1]. The new features added to the system aimed at satisfying new user requirements in line with legal obligations imposed by applicable European legislation. In addition, changes are being implemented to improve its efficiency and the quality of the data (e.g. data quality checking rules).

Bearing in mind the distributed nature of the system and its complexity a number of SSN reference documents have been agreed by MS (e.g. Interface Control Document, XML Reference Guide). These documents contain references to preparatory actions for commissioning national systems, tests during commissioning, actions during normal operational use and actions related to the further development of SSN.

The SSN Handbook, prepared by EMSA at the request of the MS, aims at linking procedures described in existing SSN documents and presenting them together in a set of control lists. The SSN Handbook does not supersede or replace any of those existing SSN documents.

The SSN handbook will assist MS seeking answers to questions such as:

- How to connect their national system to SSN;
- How to maintain a reliable connection with SSN;
- How to act in case of failures or in addressing other problems;
- How to operate within the system by providing data, requesting data or otherwise exchanging information within SafeSeaNet.

In other words the Handbook should guide MS through preparatory and development phases up to the regular operations within the system.

[1] The proceedings of workshops are regularly published at EMSA's web-site

1.2 Users

The target readers of the SSN Handbook are:

- Users working at National Competent Authority (NCA) level in the Member States; responsible for local SafeSeaNet implementation, administration and operation as well as Technical Teams (TT) responsible for the development and maintenance of the system;
- Users working at Local Competent Authority (LCA) level in the Member States (Port, PSC, Coastal Stations and others) which gather, send to SSN or store detailed information on ships' movements;

System administrators and Maritime Support Services operators of EMSA will also profit from the use of the Handbook.

1.3 How to use the Handbook?

The questions relating to SSN have been grouped in accordance with the following subject headings:

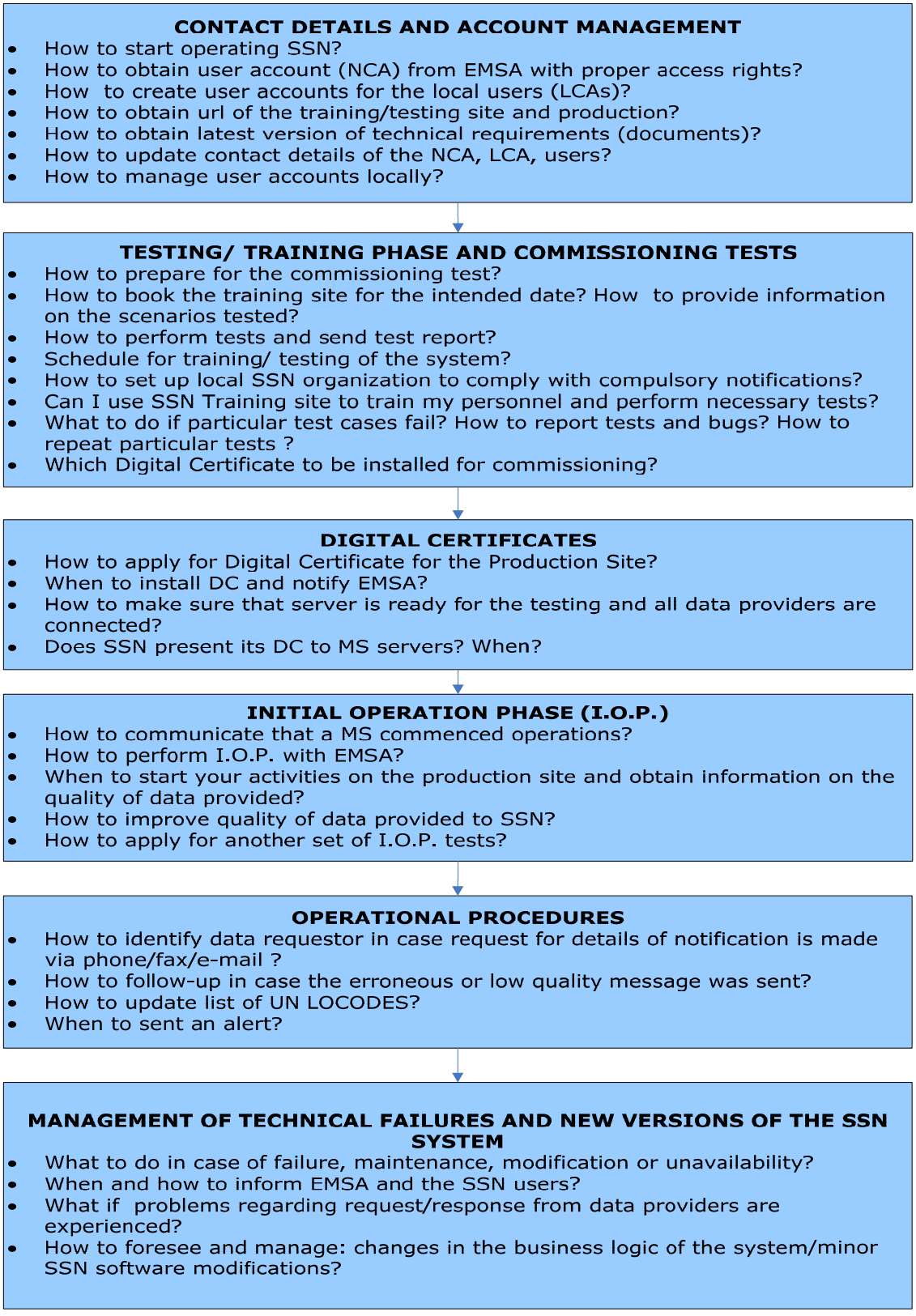
- Contact details and account management
- Testing/Training phase and Commissioning Tests
- Digital Certificate
- Start Initial Operation Phase (I.O.P)
- Operational Procedures
- Management of technical failures and New Versions of the SSN system

Additionally, each subject is subdivided into different questions. The table in part 2 of the SSN Handbook links the aforementioned subjects with control lists (in part 3).

Example of use: MS wants to change person responsible for SSN operations

- Step1: Go to page 5. Among 6 subjects presented, find the one linked to contact details.
- Step 2: While on page 5, go through different questions/issues within the subject heading. You will find a question *"How to update contact details of the NCA, LCA, and users?"*
- Step 3: Go to the part 2, page 7 of the SSN Handbook and find in the matrix table the relevant issue i.e. *"How to update contact details of the NCA, LCA, and users?"*.
- Step 4: While on page 7, in the table column "related control list" identify the relevant control list i.e.-*"1.0.1".*
- Step 5: Go to the part 3, page 16, read and follow control list 1.0.1.

Drawing - Project flow



2. Questions per subject

2.1 Contact details and account management

Questions	Related control list	Who Should apply?	Description
How to start operating SSN?	**1.0.1**	NCA, LCA	Knowledge about who is responsible for the system operations or technical management at national level can help the swift prevention/solution of problems by enabling the responsible persons to be contacted without any delay. Control lists and guidelines in this part will be used by MS to keep their SSN user accounts updated. Keeping record of valid contacts is crucial for proper operation of SafeSeaNet.
How to apply/obtain user account (NCA) from EMSA with proper access rights?			
How to create user accounts for the local users (LCAs)?			
How to obtain *url* of the training/testing site and production?			
How to obtain latest version of technical requirements (documents)?			
How to update contact details of the NCA, LCA, users?			
How to manage user accounts locally?			

2.2. Testing/ Internal training phase and commissioning tests

Questions	Related control list	Who Should apply?	Description
How to prepare for the commissioning test?	**2.0.1**	NCA, LCA	The commissioning process is required to ensure that new NCA (LCA or other SSN participant) will provide reliable, timely and accurate exchange of data, once they join the SafeSeaNet network/system with XML interface (automatic means of data transmission). This task includes control lists for all actions to MS to follow (request commissioning, who to contact, documents needed, timings, etc.); it also gives the information on the applicable documents.
How to book the "training site" for the intended date? How to provide information on the scenarios tested?			
How to perform tests and send test report?			
Schedule for training and testing of the system?			
How to set up local SSN organization to comply with compulsory notifications?			
Can I use SSN "training site" to train internally my personnel and perform necessary tests?			
What to do if particular test cases fail? How to report test results and bugs? How to repeat particular tests?	**2.0.2**		
Which Digital Certificate has to be installed for commissioning?	**3.0.1**		

2.3 Digital Certificate

Questions	Related control list	Who Should apply?	Description
How to apply for Digital Certificate for the Production Site?	**3.0.1**	NCA	Basic SSN security requirements are based on authentication, confidentiality and integrity for the secure exchange of the XML messages within SafeSeaNet. Those requirements are achieved, among other means, by application of the Digital Certificates. EMSA has a constituted procedure for MS to apply for SafeSeaNet SSL server certificates. In practical terms Digital Certificate is essential when user intends to request for data using XML and when the user acts as data provider (i.e. responds to requests made by other SSN users).
When to install DC and notify EMSA?			
How to make sure that server is ready for the testing and all data providers are connected?			
Does SSN present its DC to MS servers? When?			

2.4 Initial Operation Phase (I.O.P)

Questions	Related control list	Who Should apply?	Description
How to communicate that a MS has commenced operations?	**1.0.1**	NCA	At first stage after Commissioning EMSA will make a data quality assessment of the information provided by particular MS. This assessment will be based on the scenarios performed and checks made by EMSA. As a result, each Member state will be given a grade. It will be divided into three categories: high quality of data, average quality of data and low quality of data. This task will be performed regularly: whenever new country joins production site of SSN, once there is a modification of data provided (e.g. MS wishes to introduce Ship MRS messages) or on request from MS.
How to perform I.O.P. with EMSA?	**4.0.1**	NCA	
When to start your activities on the production site and obtain information on the quality of data provided?			
How to improve quality of data provided to SSN?			
How to apply for another set of I.O.P. tests?			

2.5 Operational Procedures

Questions	Related control list	Who Should apply?	Description
How to identify data requestor in case request for details of notification is made via phone/fax/e-mail ?	**5.0.1**	NCA, LCA	This task aims at maintaining proper protection of data i.e. that only authorised persons and entities have an access to the data to which they are entitled (phone and fax).
How to follow-up in case the erroneous or low quality message was sent?	**5.0.2**	NCA	Maritime Support Services MSS will contact data providers and request for correction or follow-up in case of detected errors or inconsistencies. Member States should consider proper reaction times for the follow-up actions
How to update the list of LOCODES?	**5.0.3**	NCA	This task describes application and use of the UNECE LOCODES in SSN.
When to send an alert?	**Alert messages guidelines (foreseen 5.0.4)**	NCA, LCA	In many cases, SSN users (LCA, MRCC, PSC, VTS or Costal Stations) are also source of alert information. In order to make sure that the alerts are send in accordance with requirements of the Directive 2002/59/EC, responsible users should apply approved version of the “SafeSeaNet Alert Messages Guidelines”.

2.6 Management of technical failures and new versions of the SSN

Questions	Related control list	Who Should apply?	Description
What to do in case of failure, maintenance, modification or unavailability?	**6.0.1**	EMSA, NCA	Once in the operations, Member States should provide proper availability of their systems interfacing SSN. In case of technical failure on MS side, there is a need to inform EMSA and other SSN users that information from particular Member states will not be available and what are alternative ways of communication in case of emergency to obtain this data.
When and how to inform EMSA, the SSN users?			
What if problems regarding request/response from data providers are experienced?			
How to foresee and manage potential system changes/modifications?	**6.0.2** **6.0.3**	EMSA, NCA	If considerable changes are introduced into SSN business logic, EMSA launches so called 'Change Management Plan'. Aim of this plan is to keep all the Member States aware of the changes that may influence their national applications. Referred control list describes the information that should be followed to Member States once the Change Management Plan is launched. Regardless the Change Management Plan, minor changes of the SSN software are also notified to Member States. In order to prepare for the new release of the SafeSeaNet the users should be aware of the possible impact on their local applications. Control Lists of this part describe code of conduct of the EMSA, NCA or Technical Teams.

3. Control Lists

EMSA	SafeSeaNet Handbook	Date: **12/09/08**
	INDEX AND FORMAT	Version: **0.02**

No.	Description	Version
0.0.0	Index and format	0.02
1.0.1	"Welcome on Board" document and update on the contact details	0.02
2.0.1	Commissioning Tests and testing/training period	0.02
2.0.2	Reporting after Commissioning Tests	0.02
3.0.1	Request for the Digital Certificate for production site	0.02
4.0.1	Entering Production Site of the SafeSeaNet, initial Operation Phase (I.O.P)	0.01
5.0.1	Operational Control List– request for information	0.02
5.0.2	Follow-up on the reported quality errors	0.02
5.0.3	LOCODES update	0.02
5.0.4	Alert Messages Guideline	X.XX
6.0.1	Technical failures – reporting and management	0.01
6.0.2	Basic information on the change management plan	0.01
6.0.3	SSN SafeSeaNet software new releases	0.02

Control List format

EMSA	SafeSeaNet Handbook	Date: **00/00/00**
	X.X.X – Title	Version: **0.00**

Structure of the control list

1. Objective

……

2. Description, responsibilities and documents linked with the control list:

WHEN TO APPLY:	**WHO SHOULD APPLY:**
• …… • …… •	• …… • ……
GENERAL INFORMATION – Familiarize your self before requesting for the WoB document	
ACTION ……	
REFERENCE DOCUMENTS	
……	

1. Objective:

To keep updated the list of persons responsible for the operations (development) of the SSN system on the National Level.

2. Description, responsibilities and documents linked with the control list:

WHEN TO APPLY:	WHO SHOULD APPLY:
• **TO START ANY OPERATION WITH SSN** • **CONTACT DETAILS HAVE CHANGED** • **OPERATIONAL CONTACT CHANGED** • **DIGITAL CERTIFICATE HAVE CHANGED** • **ONCE A YEAR, TO CONFIRM THE PERSONS RESPONSIBLE**	• **NCA, LCA**

GENERAL INFORMATION – Familiarize yourself before requesting for the WoB document

Welcome on Board document is issued by EMSA per each MS. This document formalises entering of each Member State into the SafeSeaNet system and summarises the information necessary for running MS application in the "production" and "training environment". **This document has to be filled in and forwarded to EMSA before launching any activity with SafeSeaNet.** It also has to be regularly updated as per conditions of application of this list or whenever information changes.
You will be requested to fill contact details tables in the Welcome on Board document. Weather you are commencing training/testing or wishing to join the production (real operations of the SSN) you will be asked to fill the appropriate parts of the Welcome on Board document.

Definition of contacts:

A ***Member State Representative*** at the National level is the person in charge of the general responsibility of the system. He is the Member State's representative in charge of participating to the SafeSeaNet management organisation and expressing the opinion on behalf of the Member State authority.

An Operational Contact is responsible of the management of SSN at National level. He/She is responsible for holding the complete list of documents relevant of the system and he is the contact with the EMSA team for all operational and technical issues. He will receive requests for follow-up or urgent messages provided by the MSS.

MS Contractor/ Technical contact is responsible for the technical development of SSN at MS National level, to be used in cases where the NCAs wish information to be received directly by their contractors/technical bodies, on matters relating to technical details such as improvements, changes, system failures or interruptions due to maintenance works and new releases of the SSN system.

These persons/functions have to be appointed. It is the sole authority of the Member State. All contact details must be confirmed once a year and any time there is a new version of a document issued.

REQUEST FOR THE WELCOME ON BOARD DOCUMENT	
In order to obtain or update Welcome on Board document, submit a request via email to EMSA at MaritimeSupportServices@emsa.europa.eu. EMSA (MSS) will provide you the latest version of the Welcome on Board document.	☐
If you are going to start testing or training, request from EMSA a user id, on the NCA level, to gain access to the SSN Training environment. In the other cases skip this part. The creation of the NCA user id falls under the responsibility of EMSA. Once the NCA user is created you can start sending XML messages to the SSN central system (hereinafter the European Index server – EIS) training site and you can start creating additional user ids for the LCA (CST, POR, PSC, OTH). Organization should follow the system business rules described in the ICD	☐
If you have already completed the tests/training or wish to update contact details/ accounts - request from EMSA a user id, to gain access to the SSN Production environment.	☐
Receive the WoB document from EMSA You are always required to complete/update the document and submit it back to EMSA with the following details: • The Member State representative(s). • The technical operational person(s).(Refer to the General Information section) • Technical information. Define or update the representative for the account, his/her contact details, the location, the type of network to be used (TESTA/Internet), the type of interface.	☐
If you intend to use the WEB interface only, skip this point. If you are going to use XML interface, indicate: • Data Provider URL: It is the URL pointing physically to the remote website of the Member State allowing SafeSeaNet to get the result of its request in xml format. • Data Requester URL: It is the URL pointing physically to the remote website of the Member State allowing SafeSeaNet to send the answer to a request previously sent by the Member State. • ***Provide information on the Digital Certificate (DC) installed on the National level – refer to the control list 3.0.1***	☐
Return completed document to EMSA and store the latest version at NCA level.	☐
EMSA will confirm the receipt of the documents.	☐
Consider the condition of application of this control list in your local procedures for the operations of SafeSeaNet in order to provide updates/confirmation of the contacts at least once a year.	☐
Update Welcome on Board any time there are changes in any section described in the checklist	☐
REFERENCE DOCUMENTS	
Interface Control Document (ICD), - http://www.emsa.europa.eu/Docs/ssn/ssn_icd_v1_rev0.pdf SSN v1.9 User Manual, version 1.02 - http://www.emsa.europa.eu/Docs/ssn/ssn-umn-v1.02-public.pdf	

1. Objective:

To organize and execute properly Commissioning Tests.

2. Description, responsibilities and documents linked with the control list:

WHEN TO APPLY:	WHO SHOULD APPLY:
• WHEN TRAINING YOUR PERSONNEL or WHEN IN PREPARATION FOR COMISSIONING TESTS • WHEN PREPARING COMMISSIONING TESTS • WHEN EXECUTING COMMISSIONING TESTS	• SSN CLIENT APPLICATION USERS; • MEMBERS OF THE DEVELOPMENT TESTING TEAM; • EMSA PERSONNEL THAT ARE INVOLVED WITH THE SSN PROJECT; • ANY PERSON INVOLVED IN THE DEPLOYMENT OF SSN; • ANY PERSON OPERATING THE SSN HELPDESK SERVICE.

CHOICE OF THE SCENARIOS BY NCA	
Based on the requirements of the Directive 2002/59/EC NCAs should decide on the scope of the messages provided to the SafeSeaNet system	☐
Member States are encouraged to undergo tests also at an early stage of organization foreseeing change or new development. For example at the stage of planning, future introduction of the MRS may benefit from early commissioning	☐
Organization of the SafeSeaNet on the national level should be also prepared in order to create desirable number of authorities and user accounts for the commissioning. Member State may profit in the future if test organization reflects as much as possible the real structure of the SSN locally.	☐
PREPARATORY PHASE – USER ACCOUNTS AND OTHER ISSUES	
Make sure you have produced a test environment isolated from the development and production environment. Training site may be used to test your training interface as well as for training your personnel.	☐
Request from EMSA a user id, on the NCA level to gain access to the SSN Training environment. (The creation of the NCA Authority (XML user) id falls under the responsibility of EMSA). ***Execute control list .1.0.1.***	☐
Once the NCA user is created you can start sending XML messages to the SSN central system (hereinafter the European Index server – EIS) training environment.	☐
When you decided on the timing for the Commissioning Tests, you should contact EMSA at MaritimeSupportServices@emsa.europa.eu and request **to book the training environment for the purpose of test at least 5 days prior to testing.**	☐

Create additional UserId for the LCA (CST, POR, PSC, and OTH) that will participate in SafeSeaNet. This should reproduce future foreseen organization of the SSN at the National level. Make sure you have all users created and defined.	☐
Establish and communicate to EMSA (see section "Selection of the scenarios to be executed") types of messages that have to be tested	☐
Prior commencing tests confirm with EMSA if your Digital Certificate for the training environment is properly mapped at the level of SafeSeaNet hosting environment.	☐
TOOLS REQUIRED FOR THE TESTING (Member States level and EMSA) – FOR GUIDANCE	
Member state client machine: The client machines that the NCA users use to access the system through the Internet or TESTA.	☐
EMSA: SSN Core The web server and the application server are Sun machines running the Sun Solaris v9 operating system. This is where SSN core is installed. EMSA	☐
EMSA: SSN Core Database The database server is a Sun machine running the Sun Solaris v9 operating system, where the SSN Oracle RDBMS version 9.2 is installed	☐
SELECTION OF THE SCENARIOS TO BE EXECUTED/ PRIOR TESTING	
Define the scope of the commissioning test by specifying the test scenarios to be covered. The available test cases are further extended into separate test scenarios with different input in order to trigger the validation of additional business processes extending the "normal" flow of events.	☐
Scenarios can be found in the Chapter 5 of the Member States Commissioning document : http://www.emsa.europa.eu/Docs/ssn/ssn-msctp-v1.00-public.pdf	☐
Make sure you are using proper nomenclature for the test cycle: Member State: XX, 2 letters representing the Member State, Test Phase: C (conformance testing) Test Cycle: 1 to n Test scenario id: each test scenario being provided in the last section of the Member States Commissioning document contains a test scenario id, which corresponds with the TestID proposed in the latest version of the XML Messaging Reference Guide. Examples of Test Announcement by Member States: ***PL-C1-S0111-01*** stands for The Poland Member State is executing test scenario S0111-01 during the conformance test phase, first test cycle. ***DE-C2-S0521-05*** stand for The German Member State is executing test scenario S0521-05 during the conformance test phase, second test cycle.	☐
Provide EMSA MaritimeSupportServices@emsa.europa.eu with the details of the authority that will perform the test and the user ID account that will be used and the test data (actual files).	☐
Make sure you are using the latest available version of the XSD (XML Schema Definition): http://www.emsa.europa.eu/end806d007.html	☐
Make sure your testing data will follow messages compliant with XSD (as above) and latest edition of the SafeSeaNet XML Messaging Guide: http://www.emsa.europa.eu/Docs/ssn/ssn-xmlmessagingrefguide-01_64.pdf	☐

Make sure your testing data will provide TestID uniqueness. When sending (generated) XML messages make sure you will use the 8-character representation. When announcing test activities use the extended representation. Currently the XML schema does not impose and SSN Core does not validate upper boundaries of attribute values.	☐
XML Test Message. When testing XML interface implementation, you should use your test environment (and test interface) to generate XML messages that will be send to the SSN Central System. The test interface should provide a means to enter the TestID related with the test scenario being executed. This TestID should then be incorporated into the XML message at the exact location being defined in the XML Messaging Reference Guide. The TestID consists of a sequence of 8 characters (-) included. Return XML messages from the SSN Central System will repeat the TestID. The "From" attribute reflects the sender, not the sender's location or LOCODE, nor its role. SSN Core itself will make the mapping between user, role and location code. Remember to enter always the received UserId in the "From" attribute and not your location code because a location code or location can be linked to multiple users with different roles and different access rights.	☐
Prior the testing date, Provide EMSA with the test data per Test Case/Scenario in order to validate the completeness of the tests and trace the logging information.	☐
RESPONSIBILITIES OF THE TESTING TEAM PRIOR COMMENCING TESTS – FOR GUIDANCE	
Assign roles and responsibilities of the testing team members	☐
Note testing team members coordinates and assign contact persons (internal and external)	☐
Set up test environment	☐
Make up the list of test cases and test scenarios available to EMSA (This step should follow the decision of the NCA on the scope of test)	☐
Make up list of test cases and test scenarios that will be executed, and group them into a test cycle	☐
Provide to EMSA test data (actual files) when testing the XML interface	☐
Prepare test database, and database connection, introduce test data	☐
At the date of test, contact EMSA to initiate testing	☐

RESPONSIBILITIES OF THE TESTING TEAM DURING COMMISSIONING TESTS	
Inform the EMSA at MaritimeSupportServices@emsa.europa.eu : • Who the test manager is, and if he/she acts as Single Point Of Contact -SPOC (provide name/email address/ phone) • Who the tester(s) is (provide name/email address/phone) It is relevant only for test result reporting and bug reports when extra information is required) • Who the test system admin is in case test environment problems occur (provide name/email address/phone) • When the above people are available (working hours)	☐

In return you should be notified with following information from EMSA: • Who the contact persons are for EMSA (provide email address/ phone) in terms of organisational follow-up • Who the contact persons are for hardware issues • Who the contact persons are for function testing support (scenario execution, checkpoints, result interpretation) (provide name/email address/phone) • When the above people are available (working hours)	☐
Remember, Test Support is provided for you. During a Test Phase problems could occur like connection issues, functional misunderstandings, organisational difficulties and others. In order to minimize and resolve those problems EMSA will provide a helpdesk service under following contact details: • SSN Helpdesk phone: +351 21 1209 415 from 9am (GMT+1) to5.30pm (GMT+1), Monday till Friday • SSN mailbox: MaritimeSupportServices@emsa.europa.eu	☐
Execute test cycle: • Capture test results, store results, generate report • Describe bugs encountered **REPORTING ON THE COMISSIONING TEST – EXECUTE Control List: *2.0.2 Commissioning tests reporting***	☐

REFERENCE DOCUMENTS
Member States Commissioning: http://www.emsa.europa.eu/Docs/ssn/ssn-msctp-v1.00-public.pdf SafeSeaNet XML Messaging Guide: http://www.emsa.europa.eu/Docs/ssn/ssn-xmlmessagingrefguide-01_64.pdf SafeSeaNet XSD (XML Schema Definition) can be downloaded from the: http://www.emsa.europa.eu/end806d007.html Directive 2002/59/EC: http://www.emsa.europa.eu/Docs/ssn/dir%202002%2059%20ec.pdf

1. Objective:

To assure proper reporting on the Commissioning Tests

2. Description, responsibilities and documents linked with the control list:

WHEN TO APPLY:	WHO SHOULD APPLY:
• WHEN COMMISSIONING TEST ARE COMPLETED – • WHEN BUGS OR PROBLEMS WERE ENCOUNTERED DURING COMMISSIONING	• NCA • TECHNICAL TEAMS (CONTRACTOR) • EMSA's MSS

BACKGROUND INFORMATION	
The result of the test shall be documented in a test report. It includes a test cycle reporting drafted by the test manager in accordance with the test plan and the bug report drafted by the test support contractor. The complete report and the data files (if any) shall be submitted to the SafeSeaNet mail for further evaluation and for subsequent review at the closest workshop or Member State meeting. After review of the test report, the Member States make appropriate recommendations.	☐
REPORTING OF THE COMMISSIONING TESTS	
As soon as the tests are performed and the test results are known, the following concluding steps are to be done:	☐
Download from the EMSA website http://www.emsa.europa.eu/end806d007.html the Commissioning Tests report.	☐
Make sure that you work by test cycles which should contain the following data: Name Tester, Date(s) of testing, Test Cycle Indicator, Build version being tested (mainly for local tests), Complete test list (all test scenarios provided + those added by the implementer)	☐
Forward the test report and provide feedback of bugs encountered to EMSA at MaritimeSupportServices@emsa.europa.eu	☐
Request new test cycle (if required). For example if the scope of the scenarios defined by the NCA was not successfully performed.	☐
Wait for the new edition of the Welcome on Board document sent by EMSA's MSS with the scope of the scenarios performed. Execute control list ***1.0.1 Welcome on Board document update.***	☐
Once the WoB received and updated execute control list ***4.0.1 Initial Operation Phase of operations within the SSN.***	☐
REFERENCE DOCUMENTS	
http://www.emsa.europa.eu/end806d007.html the Commissioning Tests report. http://www.emsa.europa.eu/Docs/ssn/ssn-msctp-v1.00-public.pdf - SSN Member States Commissioning	

1. Objective:

To apply for the DIGITAL CERTIFICATE necessary for notifying SSN and execute request/response.

2. Description, responsibilities and documents linked with the control list:

WHEN TO APPLY: • WHEN APPLYING FOR THE NEW DIGITAL CERTIFICATE • WHEN REQUESTING FOR THE UPDATE OF THE EXISTING CERTIFICATE	WHO SHOULD APPLY: • NCA	
DIGITAL CERTIFICATE GENERAL CONSIDERATIONS FOR ONE WAY COMMUNICATION		
To apply 1-way SSL for sending Notifications to the EIS, your server (system) must trust the GlobalSign Server Certificate on the Webgate EIS server.		☐
DIGITAL CERTIFICATE GENERAL CONSIDERATION FOR TWO WAY COMMUNICATION		
To use 2-way SSL for sending and receiving data request (MS2SSN_<type>_Req & SSN2MS_<type>_Req) and response (MS2SSN_<type>_Res & SSN2MS_<type>_Res) messages to/from the EIS. Acquire a digital certificate (***SEE SECTIONS BELOW AND CHOOSE DESIRED METHOD***) from a trusted authority and install it on the Web server interfacing with the EIS.		☐
Report to EMSA via ***WELCOME ON BOARD UPDATE CONTROL LIST 1.0.1*** your digital certificate details such as issuing company, the domain of the Web server where the certificate will be installed and the validity dates. Please attach (encrypted file) with root certificate or indicate the WEB page where it can be found.		☐
The domain of your server will be configured at the EIS Reverse Proxy level. **It is very important to note that the domain of the Data Provider and Data requester URLs given in the used id details match the domain of the digital certificate.** Also, note that if you provide Notification details in the form of electronic documents, these documents must be available over the Web server where the certificate is installed.		☐
SSN presents its DC when requesting for the details of the particular notification. Ensure you web server trusts the Root CA certificates of the EIS Reverse Proxy server.		☐
Ensure your Firewall and DNS servers are configured for the EIS Reverse Proxy server.		☐

APLYING FOR THE NEW CERTIFICATE FOR FREE VIA EMSA (MS that already possess certificates shall follow the below mentioned control list when the certificate's renewal becomes due)	
(CAUTION: SafeSeaNet Network & Security Reference Guide, Chapter 2, Procedure to apply certificate as described in the chapter, with e-trust Belgacom is not applicable and should not be used.	☐
Request EMSA MaritimeSupportServices@emsa.europa.eu for one or more web server certificates. A full justification is necessary, if more than one certificate is required.	☐
Following your request, EMSA will send a request on behalf of the MS to DG ENTR/IDABC asking for the SSL Server Certificate(s). An order for DC will be issued to Postecom.	☐
IDABC sends to Postecom the Order Form for issuing the number of certificates asked for. IDABC confirms with EMSA that the certificate(s) can be issued under the IDABC PKI and that IDABC will pay for the certificate.	☐
You should receive from EMSA necessary documents (provided by IDABC) for completion.	☐
After competition you should send the following documents in the prescribed manner, to Postecom (with a copy to IDABC): • Registration Form • Postecert Certificate WEB Server Contract • Server Responsible Appointment Module • CSR file	☐
The documentation can be transmitted to Postecom by: • Fax Registration at +39 0659585049 or +39 0659585028, or • E-mail attachment (signed documents have to be scanned into PDF files) Marilli.Rupi@postecom.it with copy to John.STIENEN@ec.europa.eu To make the transmission by E-mail more secure, the files can be stored in a Zip file archive with password protection. Please inform Postecom and IDABC about this in a proper way.	☐
After verification, Postecom will inform the you about the status of the order	☐
Once the certificate is generated, it is sent to the e-mail address of the Server's Responsible that appear in the Registration Form in Attachment 1 of the CPS. Should you discover any errors or defects in the certificate, you must inform Postecom immediately at the e-mail address Marilli.Rupi@postecom.it otherwise, the Requester will be considered to have accepted the certificate	☐
Install the digital certificate issued by Postecom on the basis of the CPS only on the web server corresponding to the domain indicated on the said certificate (in the Common Name field).	☐
If problems occur during the process, you may contact the Postecom helpdesk at: support.idabc@postecom.it	☐
Once the control list is concluded, you should inform the SSN helpdesk about the completion of the task. Report to EMSA via ***WELCOME ON BOARD UPDATE CONTROL LIST 1.0.1*** your digital certificate details.	☐

ALTERNATIVE - APLYING FOR THE NEW CERTIFICATE DIRECTLY AT A THRUSTED CERTIFICATION AUTHORITY –CA.	
You may prefer to purchase the certificate on your own, as this procedure goes smoother and faster and additional administrative work can be saved. If you choose to obtain it directly, you can get it at your national telecom or trough other trusted organizations. The cost for obtaining the certificates is around 200€ and support is provided by CA.	☐
Inform the EMSA if you intend to apply for the Digital Certificate at the national level. ***BE ADVISED THAT SELF-SIGNED CERTIFICATES ARE NOT ACCEPTED (Those are only allowed for the limited period of testing e.g. 2 weeks)***	☐
Trusted organization of your choice may require set of documents supporting your request.	☐
Once the action is concluded, you should inform the SSN helpdesk about the completion of the task. Report to EMSA via ***WELCOME ON BOARD UPDATE CONTROL LIST 1.0.1*** your digital certificate information.	☐

REFERENCE DOCUMENTS
SSN procedure on how to apply for digital certificate http://www.emsa.europa.eu/Docs/ssn/certificates-v2.10.pdf Interface Control Document (ICD), Chapter 7, System Specification : http://www.emsa.europa.eu/Docs/ssn/ssn_icd_v1_rev0.pdf SafeSeaNet Network & Security Reference Guide, Chapter 2, ***(CAUTION: Procedure to apply certificate as described in the chapter, with e-trust Belgacom is not applicable and should not be used)*** http://www.emsa.europa.eu/Docs/privssn/ssn_network_securityrefguide-01_14-en.pdf

1. Objective:

To ensure that a Member State is entering the production site of SSN with all required data. It is also to provide MSs with feedback from EMSA on what is the quality of the information provided.

2. Description, responsibilities and documents linked with the control list:

WHEN TO APPLY:	WHO SHOULD APPLY:
• WHEN MS WISHES TO JOIN PRODUCTION SITE • WHEN THERE ARE ANY CHANGES OF THE SCOPE OF INFORMTION PROVIDED FOR SSN (e.g. MS INTRODUCED ADDITIONAL AUTHORITIES) • WHEN A MS WISHES TO VERIFY QUALITY AND AVIABILITY OF THE MESSAGES PROVIDE	• NCA • Technisa responsible team • Person responsible for the operations of the SSN locally

INFORMATION FLOW	
Make sure you have executed the control list ***1.0.1. Welcome on Board document update*** and that all information on the changes, performed tests, contact details etc are recorded and updated.	☐
Inform EMSA on the data when your production server/system will commence operations with SSN EIS in order to provide notice for all SSN participants.	☐
Define information which will be provided. Confirm: Port Notification, Ship Notification (type), HAZMAT Notification (type of the response) and the Alert Notification (response type)	☐
Confirm coverage of your system (all Country, selected ports, selected authorities etc.)	☐
Make sure you are familiar with the recent changes of the SSN system. Refer to the control lists ***6.0.2 and 6.0.3 SSN New Releases***	☐
INITIAL OPERTAION PHASE and FEEDBACK ON THE QUALITY OF THE DATA PROVIDED	
Inform EMSA MaritimeSupportServices@emsa.europa.eu of the scope of the information which you would like to assess during the first week of the operations/ or any time on request: Notification type/REQ/Res type etc.	☐
After the week of the operations, you will receive information from EMSA on the results of the checks of the whole set of the selected notification type, encountered errors, and random checks of the data availability etc. Based on those findings you will receive the feedback on the quality of the information provided. It may be defined as “good quality”, “average quality” or “to be improved”. This assessment will be based on the quality and availability factors.	☐
You may use the feedback provided by EMSA in order to initiate or continue improvements of your system. This may be helpful to assess the implementation of the system as well.	☐
Prepare “lessons learnt” document. This is supposed to summarize the feedback from EMSA and to list the possible future preventive measures to avoid errors/inconsistencies. It may relate to the organization of the system (how data is inputted locally), technical implementation and relations with the data sources.	☐
If assessment is with note “to be improved”, provide information back to the MSS when errors/inconsistencies or problems will be resolved.	☐
REFERENCE DOCUMENTS	
Interface Control Document (ICD), - http://www.emsa.europa.eu/Docs/ssn/ssn_icd_v1_rev0.pdf ; SSN v1.9 User Manual, - http://www.emsa.europa.eu/Docs/ssn/ssn-umn-v1.02-public.pdf	

1. Objective:

This procedure is a code of conduct, to ensure proper transmission of information and authentication of the user when: 1. information is requested on details of HAZMAT or other notifications available via phone and fax; 2.local system failed; 3. there is a request for the details of cargo manifest (in emergency)

2. Description, responsibilities and documents linked with the control list:

WHEN TO APPLY:	WHO SHOULD APPLY:
• WHEN DETAILS OF THE PARTICULAR MESSAGE (E.G. HAZMAT) ARE AVAILABLE VIA PHONE AND FAX • WHEN REQUEST FOR DATA IS RECEIVED DURING SYSTEM UNAVAILABILITY/FAILURE/SERVICE • WHEN REQUEST FOR THE DETAILS OF CARGO MANIFEST IS RECEIVED IN EMERGENCY	• NCA, • LCA, • DESIGNATED POINT OF CONTACT 24/7

REQUEST FOR DETAILS OF MESSAGE/ CARGO MANIFEST DETAILS / REQUEST FOR VESSEL DATA IN CASE OF THE SYSTEM FAILURE	
User to request by telephone/fax/e-mail concerning details of message/ Cargo Manifest of the vessel or information on the vessel latest notifications in case of the system failure/maintenance/service	☐
Data provider to identify requestor (Country, SSN role, type of user in SSN telephone number, e-mail, fax)	☐
Confirm what is the reason of this request (routine or emergency call)	☐
Instruct requestor that if verification of his contact details is positive, information about cargo (Cargo Manifest) or the vessel latest details will be transmitted as indicated	☐
Verify information concerning calling person in SafeSeaNet1.9 (SEE BELOW) 	☐
If verification of the requestor was negative, (contact details were not matching the contacts in the SafeSeaNet) inform him/her on the result (requestor not included as contact in SSN 1.9) and confirm that information will not be forwarded. END OF ACTION/ If verification was positive go to the next point.	☐
Collect the information about cargo and send via fax/phone indicated in the SSN1.9 END OF ACTION	☐

REFERENCE DOCUMENTS
SSN v1.9 User Manual, - http://www.emsa.europa.eu/Docs/ssn/ssn-umn-v1.02-public.pdf

1. Objective:

This procedure is a code of conduct in case a request for follow-up is received from EMSA and to ensure the local system is operational as required by ICD

2. Description, responsibilities and documents linked with the procedure:

WHEN TO APPLY:	WHO SHOULD APPLY:
• WHEN REQUEST FOR THE FOLLOW –UP ACTION IS RECEIVED FROM EMSA	• NCA

GENERAL INFORMATION	
In principle EMSA will contact NCA in case of the reception of the erroneous messages (e.g. information sent successfully but not following system "business rules"; rejected messages, message sent with incorrect identifiers of the vessel, message sent with incorrect attachment for the dangerous cargo, repeated notifications of the same content, etc.). NCA is responsible for the further follow-up action on the National Level i.e. contact of the data originator (LCA) and co-ordination of the possible corrective action (technical or operational)	☐

FOLLOW –UP ACTIONS – MS LEVEL	
Identify user (entity) responsible for the transmission of the message with incorrect values	☐
Contact local responsible person / entity	☐
Investigate the nature of the problem: in case of the human error (operational issues) – skip next point	☐
If the problem relates to the technical issue (implementation, software bugs), contact your technical team to investigate. In case when messages will not be available because of the corrective action, immediately launch ***control list 6.0.1.***	☐
Request data originator sending the correction (re-sent) of the message or confirm correct values if processing of the corrective message (re-sent) is not possible (e.g. vessel has already arrived or left the port).	☐
Confirm period of the corrective action (i.e. when message with correct values will be sent) or confirm with EMSA what should be the correct data.	☐
Provide EMSA with information on the status of the follow-up action	☐
REFERENCE DOCUMENTS	
Interface Control Document (ICD), http://www.emsa.europa.eu/Docs/ssn/ssn_icd_v1_rev0.pdf	

1. Objective:

This procedure is a code of conduct, to introduce or update the list of the UNECE LOCODES used in the SafeSeaNet.

2. Description, responsibilities and documents linked with the procedure:

WHEN TO APPLY:	WHO SHOULD APPLY:
• WHEN A MS WISHES TO UPDATE THE LIST OF LOCODES	• NCA

LOCODE GENERAL INFORMATION	
LOCODE is a location defined as any named geographical place, recognized by a competent national body, either with permanent facilities used for goods movement associated with trade, and used for these purposes, or proposed by the government concerned or by a competent national or international organization for inclusion in the UN/LOCODE. In UN/LOCODE, one code element represents the name of a port, or a location, i.e. anchoring area, and in addition possible subsidiary location, i.e. an ISPS-area or -terminal. (Definition adapted from ISO 2382-4/1987) A five-character code element is provided for each location included UN/LOCODE and consists of: • two letters identifying the country, according to the ISO 3166 two-letter Code for the representation of names of countries, and UN/ECE/FAL recommendation No. 3, and • three characters identifying the location within the country.	☐
The LOCODE must be used when filing in the destination field "NextPortofCall" in the Notifications sent to SSN. The LOCODE is also a part of the identification of the Authorities in SSN and primarily it is used to identify the Port Authorities. Furthermore, every authority in SSN is assigned a LOCODE.	☐
The primary reference of LOCODEs used in SSN is the UNECE list of LOCODEs. Therefore, all the LOCODEs must be registered with UNECE. **You will receive information from EMSA, any time there is a new upload of the LOCODES list to SSN**	☐
On a temporary basis a new LOCODE can also be registered within SSN, in order to enable its use in the notifications transmitted to SSN by the NCA applications or via the SSN Web application. This LOCODE will be applicable in SSN until UNECE list is properly updated by the Member State and UNECE	☐

LOCODE UPDATE WITH UNECE	
Go to the UNECE Web site at http://apps.unece.org/unlocode/	☐
Study UN/LOCODE Manual http://www.unece.org/cefact/locode/ (Chapter 6) and follow described steps to apply for the update of the existing or introduction of the new LOCODE. If you are updating existing LOCODE, please follow steps described in the Chapter 7 of the UNLOCODE Manual.	☐

Advise EMSA MaritimeSupportServices@emsa.europa.eu on submission of your application to UNECE via e-mail:	☐
If introduction of the LOCODE on the temporary basis is required (introduction of the SSN specific LOCODE on the temporary basis), follow the steps of the next section	☐

TEMPORARY INTRODUCTION OF THE SSN SPECIFIC LOCODE	
Sent to EMSA your request for the introduction of the SSN specific LOCODE e-mail: MaritimeSupportServices@emsa.europa.eu	☐
Indicate following data: Location code, Location Name, Country and Coordinates: Longitude and Latitude	☐
You will receive a acknowledgment from EMSA when temporary LOCODE is created	☐

REFERENCE DOCUMENTS
UN LOCODE Manual http://www.unece.org/cefact/locode/. Interface Control Document (ICD), Chapter 8, UN LOCODES : http://www.emsa.europa.eu/Docs/ssn/ssn_icd_v1_rev0.pdf

Page left blank intentionally

Note: Once "Alert messages guidelines" document is approved, it will be inserted.

1. Objective:

To ensure proper information flow between data provider and users in case there is a technical failure

2. Description, responsibilities and documents linked with the control list:

WHEN TO APPLY: • DURING MAINTENANCE OF THE NATIONAL SYSTEM • UNAVAILABILITY OF THE NATIONAL SYSTEM	WHO SHOULD APPLY: • NCA • TECHNICAL TEAMS	
FAILURE or PLANNED INTERVENTION OF THE SSN SYSTEM		
Assess with your technical team type of intervention and summary of actions. Make a provisional timing for unavailability (also if result of a failure or indicate unknown time for resuming communication with SSN)		☐
Set a data and time (if intervention was planned)		☐
Inform EMSA on the intervention (if planned at least week in advance)		☐
Establish backup communication (phone/fax/mail where information maybe available on request). Depending on the level of the intervention, establish/introduce temporary procedure to use the SafeSeaNet WEB interface to provide data		☐
Request EMSA MaritimeSupportServices@emsa.europa.eu to inform all SSN participants on the period of unavailability and contact for requesting data		☐
Inform all local SafeSeaNet users on the failure/maintenance period and backup measures		☐
CONDUCT OF THE FAILURE/ INTERVENTION		
Monitor if backup communication is operational		☐
Establish constant communication with personnel responsible for the maintenance/service so as to obtain at the earliest possible stage information when the failure/ intervention is completed		☐
Make sure technical personnel will be also available when maintenance/service is completed. Make sure you are familiar with type of intervention, purpose and summary of intended actions, data and time, possible side effects of your National System.		☐
Inform EMSA MaritimeSupportServices@emsa.europa.eu and other SSN local users when your system resume operations		☐
Prepare “lessons learnt” document. This is supposed to summarize the maintenance/failure actions and to list the possible future preventive measures to avoid failures or to reduce period of the unavailability of data in case of the planned intervention		☐
CONTACTS IN THE MS FOR EMSA/ Other SSN Member States users – to be filled in by MS		
e-mail:	Phone:	☐
REFERENCE DOCUMENTS		
n.a.		

1. Objective:

To describe and explain conduct of actions in case of the major changes in the business logic of the system.

2. Description, responsibilities and documents linked with the control list:

WHEN TO APPLY:	WHO SHOULD APPLY:
• WHEN THERE IS A PREPARATION FOR THE NEW VERSION OF THE SSN RELEASE	• NCA • TECHNICAL DEVELOPERS OF THE SYSTEM • EMSA's MSS

CHANGE MANAGEMENT PLAN – BASIC INFORMATION and INITIATION	
For the purpose of this document, it is assumed that all changes of the system are agreed with Member States.	☐
The Change Management plan is applied when there is an impact for the SafeSeaNet system specification and hence to the Member State's national SafeSeaNet implementations. Changes of the following are particularly relevant: • XML Message Reference Guide • Network and Security Reference Guide • XML Schema Definition • Interface Control Document	☐
The change Management plan is not applicable to: • Changes that have no effect on the National SSN implementation • EMSA organization • Changes in the legal documents (Directives etc.)	☐
EMSA is responsible for launching change management plan. Change Management plan aims at prompt reporting to the Member States on the proposals related to SSN. In general, EMSA will provide NCA with all necessary documents that summarize the changes of the versions of SafeSeaNet. It may be also a case when a summary of changes is announced at the SafeSeaNet workshop. Clear reference to that will be provided.	☐
It is the responsibility of the MS to assess the impact of each proposal on the national SafeSeaNet implementation. Most important duty of the NCA is to communicate all the expected changes to the SafeSeaNet local users. There may be a need to consider organizational and technical impact of those changes on the National Application	☐
Once you are communicated that the Change Management Plan was launched you should receive following information: • Source of the change (follow-up of the earlier detected errors, legislative changes, etc.)	☐

• Scope of the changes (documents, manuals, environments, technical documents XML, XSD etc.) • Foreseen impact assessment • Testing and validation procedure • Planning of the changes	
Regardless of the fact, if changes were initiated based on the Change Management Plan or not, you should follow control list 5.0.2– New releases, description and announcements	☐
Referred documents	
Change management Plan http://www.emsa.europa.eu/Docs/ssn/ssn-cmf-issue1-rev0.pdf	☐

1. Objective:

To confirm actions to be taken on the local level before next software release of the SSN system

2. Description, responsibilities and documents linked with the control list:

WHEN TO APPLY:	WHO SHOULD APPLY:
• WHEN THERE IS A PREPARATION FOR THE NEW VERSION OF THE SSN RELEASE • WHEN YOU ARE IN DOUBT WHAT IS THE LATES VERION OF THE SSN SOFTWARE	• NCA • TECHNICAL DEVELOPERS OF THE SYSTEM • EMSA

SafeSeaNet release identification – basic description

SSN application releases are identified using the following scheme: <app name> <app ver> where:

- <app name> is the name of the application e.g. SNN
- <app ver> is the release version number in the format M.S.P.H where:

M - two digits, indicating the version of Major release e.g. 1.9; S- one digit, indicating the version of the Service Pack, compatible with a Major release e.g. 0; P - one digit, indicating the version of the Patch Release compatible with a Service Pack release e.g. 4; H - one digit, indicating the version of the Hot Fix compatible with a Patch release e.g. 4 - The SSN application release, for instance, is identified by SSN 1.9.0.4.4.

The releases are classified into *Major, Service Pack and Emergency software fixes* with the following characteristics:

- Major software release upgrades, normally containing large areas of new functionality, some of which may make intervening fixes to Problems redundant. A major upgrade or release usually supersedes all preceding Service Packs, Patch Releases or Hot Fixes.
- Service Pack release upgrades, normally containing small enhancements and fixes, some of which may have already been issued as emergency fixes. A Service Pack upgrade usually supersedes all preceding Patch Releases or Hot Fixes.
- Emergency software fixes, normally containing the corrections to a small number of known Problems.

The final approval of a release or planned system maintenance to the Training or Production environments is given by EMSA.

Reporting on the SSN releases (Major and Service packs) and future planning is communicated to SSN Participants during the SSN workshops

An email notification is foreseen to the SSN Participants prior to each release while a last confirmation is also communicated by email on the date of the new release installation on the TRAINING and PRODUCTION environments.

The yearly planning of new releases will be communicated to the Member states during the SSN workshops or the announcement of a Major Release will be communicated at least 6 months in advance and prior to the installation on the SSN Production environment.

Service pack will be communicated at least 2 months in advance and prior to the installation on the SSN

Production environment.
Patch Releases and Hot Fixes must be communicated to the SSN Participants at least 2 weeks in advance and prior to the installation on the SSN Production environment. NOTE: Patch Releases and Hot Fixes do not include any changes to the specifications and thus do not affect the XML protocol that the NCA SSN client systems use to interface with SSN Central and thus have a minor impact to the Member States.

ANNOUNCEMENTS – TIMING **This section defines the timing when particular message will be announce to you. This is supposed to give NCAs time to organize support team if required or to confirm activities with contractor's group.**	
Information on Major Release: Will be forwarded 6 months prior to the installation on the SSN Production environment. Communication: SSN Implementation Plan report submitted during the workshops followed by an email broadcast. Originator of the message: EMSA Recipients: (All groups) Member State Representative Group, Operational Group, Member state Contractors Group **Make sure your support team is organized for the due date**	☐
Information on Service pack release: You will be informed 2 months prior to the installation on the SSN Production environment. Communication: Email Initiator: EMSA Recipients: Operational Group, Member state Contractors Group. **Update your contractor/ support team**	☐
Upon release of the Patches and Hot Fixes: You will be notified 2 weeks in advance and prior to the installation on the SSN Production environment. Communication: Email broadcast. Initiator: EMSA Recipients: Operational Group, Member state Contractors Group. **Update your contractor/ support team**	☐
Following reception of any of the messages, liaison with contractor/ technical support as per further sections: **Change on the Production Site/ Change of the training Site**	☐

Reminder Alert (all type of releases): When the new release is ready to be installed on the Training environment and at least 2 weeks prior to the installation on the Production environment. To be broadcasted by an email. Communication medium: Email broadcast. Initiator: EMSA Recipients: Operational Group, Member state Contractors Group. **Make sure your contractor / support team is informed**	☐
Final Reminder Alert (all type of releases): 24 hours prior to the installation on the Production environment. Communication medium: Email broadcast. Initiator: EMSA Recipients: Operational Group, Member state Contractors Group. **Update your contractor / support team**	☐
Announcement of Delays: (All type of releases): Any delays or changes to the planning must be communicated to all the Member States in due time together with a justification for the delay/change. Communication medium: Email broadcast. Initiator: EMSA Recipients: Operational Group, Member state Contractors Group. **Make sure your contractor / support team is informed on delays**	☐
Release notes and updated release notes (all type of releases): The release notes stating all the applied changes and incidents/bugs resolved will accompany every new release. In addition following information will be provided: a) the list of documents affected b) any known bugs will be reported in a distinct form to be included in the release notes document. The release notes will be broadcasted by email to the list of recipients and will be published via the EMSA Web site at: http://www.emsa.europa.eu/end806d007.html **Make sure you are familiar with the list of documents affected and list of bugs, which will be corrected. Communicate changes to the support team / contractor**	☐

Announcement Email Format. **The email to be broadcasted announcing a new release will specify:** • The version of the new release and the classification to Major/Service Pack/Patch Release/Hot Fix. • The scope with a summary of the major functional elements affected. • The environment where the release will be installed. • The foreseen date/time of the release and were applicable the duration of the intervention (installation). • The release notes. Upon completion of the installation of a new release, the helpdesk/EMSA will broadcast a confirmation email. **Check if the information received by you is complete**	☐

Changes of the TRAINING site of the SSN	
NOTE: This procedure may also be applied if you are willing to participate in the testing process of the new version before deployment. In that case, you will be able to test new version of the SSN software on the training site before it is deployed on the production site.	
Received information on the update for SSN Training site version of SSN, if not request EMSA and provide it to all parties involved in the SSN (LCA, Contractors)	☐
Received url addresses of the Training Site, if not request EMSA for update	☐
Confirm user accounts for the SSN Training Site (***Execute 1.0.1 Welcome on Board update control list if required***). If problems with LOGIN, PASSWORD request EMSA for checks	☐
Confirm the reception of the list of changes/ assess impact on technical organizational. Make sure you are familiar with: type of intervention, purpose and summary of intended actions, data and time, possible side effects	☐
Set a date for the organization change, if required – if outside the planned introduction of the new production release, inform EMSA	☐
Set a date for the technical change, if required – if outside the planned introduction of the new production release, inform EMSA	☐
Changes of the PRODUCTION Site of the SSN	
Received update of the SSN Production site version of SSN, if not request EMSA and provide it to all parties involved in the SSN (LCA, Contractors)	☐
Received date of the implementation of Production new version – if not request EMSA for confirmation	☐

Make sure technical personnel available (Member state technical or contractor group) for the switch over of the local system. It may require a controlled server shutdown. Make sure you are familiar with: type of intervention, purpose and summary of intended actions, data and time, possible side effect	☐
Inform other SSN local users on the period of unavailability of the Production Site and your schedule of local implementation.	☐
On the date of the switch over, contact with the responsible technical personnel available (Member state technical or contractor group) - confirm the successful switch over to new version. If you experience any technical problems, obtain possible schedule of the problem solution and inform EMSA	☐
Inform testing group / designated persons on the testing phase period, if any errors problems, request EMSA for investigation	☐
Referred documents	
n.a.	

Annex

Abbreviations and Acronyms

CST	Coastal Station
DC	Digital Certificate
EC	European Commission
EIS/SSN Core	European Index Server/SafeSeaNet System Core application -
EMSA	European Maritime Safety Agency
ETA	Estimated Time of Arrival
ETD	Estimated Time of Departure
GUI	Graphical User Interface
HAZMAT	Dangerous or Polluting Goods
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL
ICD	Interface Control Document
Intertanko	International Association of Independent Tanker Owners
ISPS	International Ship and Port Facility Security Code
IT	Information Technology
LCA	Local Competent Authority
MS	Member State(s)
MSS	Maritime Support Services
NCA	National Competent Authority
NCP	National Contact Point
PMoU	Paris Memorandum of Understanding
SHT	Single Hull Tanker
SLA	Service Level Agreement
SSL	Secure Sockets Layer
SSN	SafeSeaNet
TT	Technical teams
UN LOCODES	United Nations Code for Trade and Transport Locations
UserId	User Identification
WoB	Welcome on Board document
XSD	XML Schema Definition
XML	Extensible Markup Language

No	Reference	Title
1	Directive 2002/59/EC	Establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC
2	Directive 2000/59/EC	On port reception facilities for ship-generated waste and cargo residues
3	Directive 95/21/EC (as amended)	concerning the enforcement, in respect of shipping using Community ports and sailing in the waters under the jurisdiction of the Member States, of international standards for ship safety, pollution prevention and shipboard living and working conditions (Port State Control)
4	Regulation (EC) No 725/2004	On enhancing ship and port facility security
5	Regulation 1406/2002 (as amended)	Establishing a European Maritime Safety Agency
6	Regulation (EC) 1726/2003, 417/2002 and 453/2007	Accelerating phasing-in of double-hull or equivalent design requirements for single – hull oil tankers

Specific SSN documents

No	Reference / Title	Version
9	ICD / Interface Control Document	1, rev 0
10	XML SSN XMRG / XML Messaging Reference Guide	1.64
11	SSN NSRG / Network and Security Reference Guide	1.14
12	SSN CMF / Change Management Framework	1, rev 0
13	SSN UM / User Manual	1.9
14	SHT / Single Hull Tanker List	-