European Maritime Safety Agency

Ref. Ares(2022)1517929 - 01/03/2022

SafeSeaNet Common

Operational Procedures

Version: 2.2

Date: 22/11/2021

Document Approval

	Name	Date	Signature
Prepared by:	EMSA	02/10/2021	
Validated by:	SSN Group	20/10/2021	
Quality control by:	EMSA		
Approved by:	High Level Steering Group (HLSG)	08/12/2021	

Document History

Version	Date	Changes	Prepared	Approved
2.0	02.12.2014	Final version to be published	CWG	HLSG
2.1	20.06.2016	Inclusion of the timing for announcing SSN releases to MSs in Procedure 2.1	EMSA	HLSG
2.2	08.05.2020 22/11/2021	Inclusion of the AIS data retransmission procedure 2.13 Changes in line with SSN v5.0	EMSA	HLSG

Document information

Creation file	22/11/2021
Filename	SSN Common Operational Procedures
Location	http://emsa.europa.eu/ssn-main/documents.html
Number of pages	46

Table of Contents

1. Introduction

What?

This document contains procedures which shall be maintained by both national and central SafeSeaNet (SSN) systems to ensure the correct operation of the system and its mandatory functionalities, as defined in Chapter 2.3 of the Interface and Functionalities Control Document - IFCD.

When?

Procedures included in this document shall be applied for the actions which affect different types of SSN users, in specific situations. Chapter 5.3 of the IFCD includes a non-exhaustive list of procedures. This document covers the following procedures:

- Reporting technical failures or planned interventions / releases
- Providing information during system failures or planned interventions or once the routine information is available via phone and fax
- Distributing Incident Report notifications to other MSs
- Reception of Distributed Incident Reports
- LOCODEs Management
- Updating the list of SSN contact details
- Missing or mismatched Information in SSN
- Requesting and providing historical data and other types of data
- Single Hull Tankers early warning
- Communication Procedure
- SafeSeaNet central system switch to the Business Continuity Facility (BCF)
- Fail-over of a national SSN system or a national/regional AIS server

Why?

The procedures mentioned above shall support the operational services defined in Chapter 5.2 of the IFCD.

Who?

This document is intended for the following SSN users, as defined in the Chapter 1.4 of the IFCD:

- National Competent Authority (NCA)
- Local Competent Authorities (LCA)
- NCA 24/7
- Maritime Support Services (MSS)

How?

The operational procedures[1] shall 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 (IFCD Chapter 5.3).

[1] Operational procedures which only affect national SSN systems should be defined at national level and are not covered by this document.

2. Procedures

EXPLANATORY NOTE - All procedures included in the document have the following structured sections:

What Describes the purpose of the procedure as defined in Chapter 5.3 of the IFCD

When Presents the conditions for using the procedures. One or more cases* might be envisaged

Why Clarifies the procedures’ legal background. The relevant Articles of Directive 2002/59/EC are recalled as well as the relevant sections of the IFCD

Who Provides the responsible actors executing the procedure

How The relevant cases* are detailed to describe actions, responsibilities and reaction time within the procedures.

Relation to other procedures

A reference to other applicable procedure(s) is made.

*The above mentioned specific cases, detailed actions and timelines are explained further in two columns:

Explaining when Which action shall be performed and by who.

Templates In some cases they are provided in some procedures to facilitate the communication between the MSs and EMSA MSS or in order to harmonize and facilitate the information exchange.

2.1 Reporting technical failures or planned interventions/releases

What 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 (Central SSN system or National SSN system including its local components).

The Central SSN planned interventions/releases are classified into Major, Minor 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 Minor, Emergency software fixes.
- Minor software releases upgrade, normally containing small enhancements and fixes, some of which may have already been issued as emergency fixes. A minor software release can have minor effects on the XML Messaging Reference Guide. A Minor upgrade usually supersedes all preceding Emergency software fixes.
- Emergency software fixes, normally containing the corrections to a small number of known problems. Emergency software 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.

The final approval of a Central SSN release or planned intervention to the Training or Production environment is given by EMSA.

When Three possible cases are envisaged:

I. A National SSN or the Central SSN system is unavailable due to a failure. It will not provide one, or all, of the mandatory functionalities described in the IFCD.

II. A National SSN or the Central SSN system will be under maintenance/ upgrade/service. It will not provide one, or all, of the mandatory functionalities described in the IFCD.

III. Member State receives a notification of the unavailability of a National SSN or the Central SSN system (due to a failure or a planned technical intervention).

Why Directive 2002/59/EC, Art. 22a; IFCD Chapters; 2.3, 4.1, 4.4, 5.2 and 5.3.

SafeSeaNet is a cooperative system, consisting of Member States' National systems and the Central SSN system. Once any of its components is unavailable, the system will not provide the necessary information required to support the mandatory system functionalities (IFCD 2.3) and to meet the objectives of SSN (IFCD 2.2). Moreover, other EU maritime systems, which rely on SSN information (e.g. THETIS), will be unable to function efficiently.

According to IFCD Chapter 4.3 the SSN system (Central and National) shall be maintained at a minimum of 99% over a period of one year, with the maximum permissible period of interruption of 12 hours.

Who NCA and the EMSA/MSS are responsible for implementing this procedure.

EMSA/MSS system administrators and all SSN users shall be aware of this procedure and the actions.

How See specific Cases I – II - III on the following pages.

Relation to other procedures

24/7 Backup communication procedure (2.2) Shall be put in place to make sure that data is available by alternative means of communication once the system is unavailable.

Communication procedure (2.10) Shall be put in place to ensure the proper identification/authentication between MSs or between MSs and EMSA MSS when using communication means such as phone or email.

Business Continuity procedure (2.11) Shall be executed in order to maintain the obligatory availability of the Central or National SSN system components.

Case I: Failure of a National SSN or the SSN Central system

Time/When?	I.1. NCA
A failure is detected at National SSN	A. NCA shall perform a situation analysis, assess type, actions and an outage prevision as well as identify the mandatory system functionalities impacted.
As soon as possible	B. 24/7 communication back-up procedure shall be established (see procedure 2.2).
As soon as possible	C. EMSA/MSS shall be informed by the NCA about: the provisional timing for unavailability, mandatory system functionalities impacted and backup communication procedure established; to disseminate this information to other Member States via the EMSA Portal (“News”).
As soon as possible	D. NCA shall inform all their national SSN users on the failure of the National SSN and the back-up communication procedure established.
When considered necessary	E. NCA may establish/introduce temporary procedures to provide data or to switch the National SSN system to the business continuity facility (see procedure 2.12).
Continuously	F. NCA shall monitor outage evolution and availability of back-up communication service.
After the system recovers	G. Notifications not provided during the outage must be stored and sent when failure is resolved and the operations of SSN systems resumes.
After the system recovers	H. NCA shall inform its SSN users and the EMSA/MSS on the system recovery.
Following the failure	I. Problem analyses shall be performed on the national level in order to understand the root cause and prevent reoccurrence of the failures.

Time/When?	I.2. EMSA/MSS
After a failure is detected at Central SSN	A. EMSA/MSS shall perform a situation analysis (assess type, actions and an outage prevision as well as the mandatory system functionalities impacted).
As soon as a failure is notified by NCA or after detecting failure at Central SSN	B. EMSA/MSS shall disseminate the information to all Member States (all SSN NCAs and NCAs 24/7 contacts) about: the failure of a National SSN (as reported in point I.1.C); or the SSN Central system, the mandatory system functionalities impacted and the back-up communication procedures established. Failures affecting the SSN central system shall be communicated via the EMSA Portal (“News”) and email.
Continuously	C. EMSA/MSS shall monitor outage evolution.
After the system recovers	D. EMSA/MSS shall disseminate information about a National SSN or the SSN Central system recovery to all Member States (all SSN NCAs and NCAs 24/7 contacts).

After the Central SSN system recovers	E. Problem analyses shall be performed on the Central SSN level in order to understand the root cause and prevent reoccurrence of the failures.

Case II: Planned intervention on a National SSN or the SSN Central system

Time/When?	**II.1. NCA**
When an intervention is planned at National SSN	A. NCA shall identify the duration of the planned intervention and the mandatory system functionalities impacted.
When an intervention is planned	B. 24/7 communication back-up procedure shall be planned and established during the downtime (see procedure 2.2).
When an intervention is planned	C. Depending on the timing of the planned intervention, NCA may establish/introduce temporary procedure to provide data or to switch the National SSN system to the business continuity facility (see procedure 2.12).
One week before + 1 day before	D. EMSA/MSS shall be informed by the NCA about: timing for the planned intervention, mandatory system functionalities impacted and backup communication procedures established to disseminate this information to all Member States via the EMSA Portal ("News ").
One week before	E. NCA shall inform all national SSN users on the intervention/ interruption of the National SSN and the back-up communication procedure established.
Continuously	F. NCA shall monitor the intervention evolution and availability of a back-up communication.
Once the intervention is completed	G. Notifications not provided during the intervention must be stored and sent when operations resume, as per IFCD requirements.
Once the intervention is completed	H. NCA shall inform its SSN users and the EMSA/MSS once the intervention is completed and the system resumed normal operations.

Time/When?	**II.2. EMSA/MSS**
When an intervention is planned at Central SSN	A. Major and Minor releases and future planning is communicated to SSN participants during the SSN workshops. All releases are deployed in the Training environment prior to the deployment in the Production environment.
When a Major intervention is planned at Central SSN	B. EMSA/MSS will provide 6 months prior to the installation on the SSN Production environment the technical specifications (i.e. XML Messaging Reference Guide and Schema).

When a Minor intervention is planned at Central SSN	C. EMSA/MSS will provide 2 months prior to the installation on the SSN Production environment the technical specifications (i.e. XML Messaging Reference Guide and Schema).
When an Emergency intervention is planned at Central SSN	D. EMSA/MSS will communicate 2 weeks prior to the installation on the SSN Production environment.
When an intervention is planned at Central SSN	E. EMSA/MSS shall identify the mandatory system functionalities impacted.
One week before + and 1 day before for all type of releases	F. EMSA/MSS shall disseminate the information to all Member States (SSN NCAs and NCAs 24/7 contacts) about timing for the planned intervention of the Central SSN system (Training and Production environment), mandatory system functionalities impacted and the back-up communication procedures established. Planned interventions affecting the SSN central system shall be communicated via the EMSA Portal (“News”) and email.
Once the intervention is completed	G. EMSA/MSS shall disseminate information that intervention is completed and a National SSN or the SSN Central system resumed normal operations to all Member States (all SSN NCAs and NCAs 24/7 contacts).
Continuously	H. EMSA/MSS shall monitor the intervention evolution.

Case III: MS receives a notification of a National SSN or the Central SSN system unavailability

Time/When?	**III.1. NCA**
When an intervention or a failure is notified by EMSA/MSS	A. NCA shall inform all national SSN users about: the downtime (due to a failure or intervention) of the Central SSN or a National SSN, mandatory system functionalities impacted and the back-up communication procedures established.
Continuously	B. NCA shall monitor the intervention evolution.
Once the Central SSN resumes operations	C. Notifications not provided during the intervention to the central SSN system must be re-sent when operations resume.
Once the intervention is completed or failure resumed at Central or National SSN	D. NCA shall inform its SSN users that the Central SSN or a National SSN resumed normal operations.

2.2 24/7 Communication procedure - Providing information during system failures or planned interventions or once the routine information is available via phone and fax

What

The purpose of this procedure is to ensure that a communication procedure is established and SSN users are able to request information kept at national level using alternative (back-up) communication means like phone, fax and email.

When

When a detailed SSN information was indicated by a Member State as available via phone, fax or email communication (e.g. for the cargo manifest data and the exemption information); or

When data is unavailable via SSN electronic exchange due to a technical failure at the data provider site (of another Member State) and a SSN user requires information during a maritime emergency.

Why

Directive 2002/59/EC, Art. 22a; IFCD Chapters; 2.3; 4.1 and 4.7.

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

SSN users should receive the desired information from SSN even if the electronic exchange of data is unavailable due to a failure or an intervention. In the case of phone, fax or email, they should receive the requested information within 60 minutes. This timeline is not applicable to archived information.

LCAs are free to exchange SSN information directly, but only the procedure via NCAs guarantees the proper checking of access rights, a 24/7 response and a service in English.

Who

Any SSN user not receiving the requested information via SafeSeaNet electronic information exchange.
NCA or equivalent notified about the non-responsiveness of the SafeSeaNet system.
NCA providing a requested data by alternative means (phone, email and fax)
EMSA/MSS (as a back-up solution)

How

See specific Cases on the following pages.

Relation to other procedures

Reporting technical failures or interventions (2.1)

Shall be put in place to ensure that SSN users are properly informed on technical failures or planned interventions at Central or National SSN.

Communication procedure (2.10)

Shall be put in place to ensure the proper identification/authentication between Member States or between Member States and EMSA MSS when using communication means such as phone, fax or email.

Case I: SSN user requesting for data which is not available via electronic means

Time/When?	I.1. NCA experiencing a failure or a planned intervention or holding the detailed information via phone, fax or email communication (e.g. cargo manifest)
Following a failure or when an intervention is planned	A. NCA shall execute actions described in procedure 2.1 and establish a 24/7 back-up communication, where the SSN National information could be made available by phone, fax or email, on request from other NCAs, during maritime emergencies.
When receiving the request from another SSN NCA	B. NCA shall obtain the requested data from the national system (services) and provide it to the requestor using the alternative (back-up) means i.e. phone, fax or email; within 60 minutes following the reception of the request.

Time/When?	I.2. SSN User
When information is not available via SSN by electronic means	A. A SSN user shall contact its NCA or equivalent entity to notify the unavailability of the requested information by electronic means via SSN.
After requesting SSN data	B. The requester shall await the response from the NCA or the EMSA/MSS which shall be received within 60 minutes.

Time/When?	I.3. NCA
Once user requests for SSN data or notifies data unavailability	A. NCA shall receive the information and confirm whether the failure or an intervention has been announced by the EMSA/MSS as per procedure 2.1. and whether the back-up communication procedure (phone, fax, email) has been established.
After receiving the request from the SSN user	B. NCA shall confirm which Member State holds the SSN data and immediately contact the responsible NCA of the Member State forwarding the user's request for data
In case a failure or intervention has not been announced	C. NCA shall immediately forward the requested data to the EMSA/MSS

Time/When?	I.4. EMSA/MSS
When receiving a request from another SSN NCA	A. EMSA/MSS shall confirm whether a failure or an intervention has been announced as per procedure 2.1, and in case it has not been announced, they shall contact the NCA of the Member State holding the information requesting: (1) the specified SSN data; and (2) execution of the actions as per procedure 2.1.

Case II: Distributed incident report cannot be forwarded by central SSN to the SSN NCA system of a MS via electronic means

Time/When?	II.1. NCA experiencing a failure or a planned intervention
Following a failure or when an intervention is planned	A. NCA shall execute actions described in procedure 2.1 and establish a 24/7 back-up communication, where the SSN National may receive the distributed Incident Report by phone, fax or email, on request from other NCAs, during maritime emergencies.
When receiving the distributed Incident Report from another SSN NCA	B. NCA shall receive the distributed Incident Report from another SSN NCA (via EMSA MSS) and shall internally distribute the information to the LCAs in line with procedure 2.4.

Time/When?	II.4. EMSA/MSS
When detecting that a distributed Incident Report cannot be forwarded	A. EMSA/MSS shall confirm whether a failure or an intervention has been announced as per procedure 2.1, and in case it has not been announced, they shall contact the NCA of the Member State to whom Incident Report was distributed requesting the execution of the actions as per procedure 2.1. B. EMSA/MSS shall confirm that the Central SSN has distributed the Incident Report by email to the SSN NCA system associated email address and to the SSN NCA 24/7 email in case the S2S distribution fails.

Case III: SSN user requesting information on exemption which is available via contact details

Time/When?	III.1. SSN User
When information on an exemption is needed which is available via contact details	A. A SSN user shall contact its NCA in line with procedure 2.10 to request information on an exemption available in Central SSN. SSN user / LCAs are free to exchange information directly, but only the procedure 2.10 via NCAs can guarantee the proper checking of access rights and a 24/7 response.
After requesting SSN data	B. The requester shall await the response from the NCA which shall be received <u>within 60 minutes</u>. For exemptions of type waste (i.e. waste notification, waste fee and waste delivery), Directive EU 2019/883 does not require the company to establish a procedure/internal system to provide the information on 24/7, the response time during non-working hours may be longer.

Time/When?	III.2. NCA
Once SSN user requests for exemption information	A. NCA shall receive the request for additional information regarding an exemption in Central SSN and authenticate the SSN User as per procedure 2.10.
After receiving the request from the SSN user	B. NCA shall confirm contact details associated to the exemption information and immediately contact them requesting additional information on the exemption. The provided response is forwarded to the SSN user.

2.3 Distributing Incident Report notifications to other MSs

What

The purpose of this procedure is to harmonise the process of distributing and storing information on Incident Reports.

When

When a Member State receives a notification of an incident or an accident at sea that shall be distributed to other Member States.

Why

Directive 2002/59/EC, Art. 22a, Art. 16; IFCD Chapters; 2.3; 4.2.
Incident Notifications should support 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, allows earlier precautionary actions and risk mitigation at sea by coastal states.

Who

Any Member State receiving the notification of the incident or accident at sea.

How

See specific Case I on the following pages[2].

Relation to other procedures

Reception of Distributed Incident Reports procedures and follow up actions (2.4)

Shall be executed at the National level to ensure a proper information flow for the distribution of incident reports at the national level.

[2] Further detailed information of Incident Report can be found in the "Incident Report Guidelines" available at the link: http://emsa.europa.eu/ssn-main/documents.html

Case I: Member State receives the notification of an incident / accident at sea

Time/When?	**I.1. Competent Authority receiving the notification of the incident or accident at sea (e.g. from the ship's master)**
When receiving a notification of an incident or accident at sea	A. The competent authority shall assess whether the incident report should be distributed or not and decide on the distribution list taking into consideration the provisions of the SSN "Incident Report Guidelines".
If the notification shall be distributed to other Member States	B. The competent authority can use the Central SSN Web Interface[3] or the National SSN system to distribute the notification (if compliant to the new IR protocol). The "Incident Reports distribution tool" in the Central SSN Web Interface supports the identification of the Member States along the planned route of the ship.
If the incident or accident ship's flag belongs to the EU	C. The flag Member State shall also be informed about the accident/incident reported as per I.1.A.
When appropriate	D. The competent authority can request other Member States to carry out inspections or verifications using the Central SSN Web Interface or the National SSN system (if compliant to the new IR protocol).

[3] Additional information can be found in the "Central SSN User Interface Manual" available at the link: http://emsa.europa.eu/ssn-main/documents.html

2.4 Reception of distributed Incident Report notifications and follow up actions

What The purpose of this procedure is to ensure the proper information flow for the distribution of incident reports.

When When a competent authority of a Member State receives a distributed incident report from another Member State, or

When there is an inspection or verification carried out following a notification of an incident/accident.

Why Directive 2002/59/EC, Art. 22a, Art. 16; IFCD Chapters; 2.3; 4.2; 5.2.1.

Member States shall ensure that effective exchange of the information referred to in the SSN legal framework takes place at national level, making sure that the Incident Reports received from another Member State via SSN are distributed among the relevant LCAs within the Member State.

Incident Notifications should support 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, allows earlier precautionary actions and risk mitigation at sea by coastal states.

Who Any Member State receiving the notification of the incident or accident at sea.

How See specific Case I on the following pages[4].

Relation to other procedures

Distributing Incident Report notifications to other MSs Procedure

(2.3)

Member States shall ensure that information on incidents and accidents is distributed among the relevant Member States (along the planned route of the ships involved or to the concerned Member States).

[4] Further detailed information of Incident Report can be found in the “Incident Report guidelines” available at the link: http://emsa.europa.eu/ssn-main/documents.html

Case I: a distributed Incident Report is received by a Member State

Time/When?	I.1. Competent Authority receiving the distributed Incident Report through SSN
When a distributed incident is received	A. If requested by the sender, the competent Authority shall acknowledge the reception of the distributed incident report. The competent Authority shall assess the content of the distributed Incident Report.
After analysing the content of the received incident notification	B. The authority shall internally distribute the information to the LCAs (e.g. MRCC, relevant ports, PSC, counter pollution services and any additional relevant LCAs/coastal stations), based on the national procedures. The SSN "Incident Report Guidelines" shall be used as a reference. It has to be noted that inspections or verifications in its ports can be carried out either on its own initiative or at the request of another Member State through a distributed Incident Report.
If there was an inspection carried following the notification of an incident or accident	C. The authority shall provide the results of the inspection using the SSN system (e.g. reporting the feedback). The SSN "Incident Report Guidelines" shall be used as a reference.

2.5 LOCODE management

What

The purpose of this procedure is to manage the reference list of LOCODES in the SSN system.[5]

When

When an NCA receives the list of LOCODEs detected as temporary, invalid, not permitted, non-activated locations or not-synchronized with THETIS (PSC system) or detects such locations at National level.

When an NCA is informed by an external party about the temporary, invalid, not permitted, non-activated locations or not-synchronized with THETIS.

Why

Directive 2002/59/EC, Art. 22a; annex III 2.1.1 Chapters; 2.3, 5.2.3;

Administration of UNECE locations' codes (LOCODES) is a mandatory system functionality.
Location codes allow unambiguous identification of a port.

It should be noted that each Member State is responsible for maintaining up to date lists of its own active ports, and proposing any new named geographical places as locations for inclusion in the UNECE LOCODE list.

Who

NCA when receiving the list of LOCODEs (temporary, invalid, not permitted, non-activated or not-synchronized with THETIS).

EMSA/MSS – administrator of the SSN system and the reference databases.

How

See specific Case I on the following pages[6].

Relation to other procedures

Communication procedure

(2.10)

Shall be put in place to ensure the proper identification/authentication between MSs or between Member States and EMSA MSS when using communication means such as phone, fax or email.

[5] THE SSN LOCODES Guidelines explicates the LOCODES management in SSN and is available at: http://emsa.europa.eu/ssn-main/documents.html

[6] Further detailed information of LOCODE management can be found in the "LOCODE Guidelines" available at the link: http://emsa.europa.eu/ssn-main/documents.html

Case I: NCA has been notified about the temporary, invalid, not permitted, non-activated or not-synchronized with THETIS

Time/When?	I.1. NCA
When SSN or EMSA/MSS notifies the data provider that temporary or invalid LOCODEs have been quoted in a notification	A. NCA shall verify the locations detected/reported/sent in the notifications.
Following the validation	B. NCA shall determine whether the specific location(s) are necessary for SSN reporting purposes, and thus shall be added as “Temporary” or ‘SSN specific’ or if they shall be deactivated. The **SSN LOCODEs Guidelines** shall be used as a reference document during this verification.
Following the validation	C. NCA may update the location by its own means, using the Central SSN Web interface, or request EMSA MSS to perform those actions (especially when the number of updates is considerable). In the latter case the following minimum set of data shall be provided: the LOCODE, the official location name, and the position (geographical coordinates).

Time/When?	I.2. EMSA MSS
When receiving a request from the NCA	A. EMSA MSS shall update the list based on information from Member States, deactivating the LOCODE if it was incorrect, or creating an SSN Specific LOCODE(s).

2.6 Updating the list of SSN contact details

What The purpose of this procedure is to maintain an updated list of NCA and LCA details, as well as the NCA 24/7 contact and other SSN users related to the management of the SSN system like e.g. representatives, operational contacts or contractors.

When When the SSN list of contacts has to be updated due to changes or rotation of personnel in the authorities.

When the NCA is notified of inconsistencies, problems and/or errors in the SSN contact list.

When NCA is requested to validate the existing lists on a yearly basis.

Why Directive 2002/59/EC, Art. 22a; IFCD Chapters 3.1, 3.3

The list of contacts has a crucial importance for the communication procedure and the authentication of the SSN users for procedures 2.1 and 2.10.

It is important to keep the list of contacts updated because of the distribution of information related to procedure 2.1 but also in respect of the Change Management Framework (deployment of the new software releases) in the SSN system.

Who NCAs

EMSA MSS

How See specific Case I on the following pages.

Relation to other procedures

Reporting technical failures or planned interventions procedure

(2.1)

Shall be put in place to ensure that SSN users are properly informed on technical failures or planned interventions at Central or National SSN.

Communication procedure

(2.10)

Shall be put in place to ensure the proper identification/authentication between Member States or between Member States and EMSA MSS when using communication means such as phone or email.

Case I: NCA updating the SSN contact list

Time/When?	I.1. NCA
When SSN contacts have to be updated following rotation of the personnel	A. An update shall be made to the 'Welcome on Board' document which is the official template used for notifying changes in the SSN list of contacts: SSN or NCA representatives, NCA 24/7, operational contacts or contractors. This document shall subsequently be sent to the EMSA MSS. Additionally, the NCA shall use the SSN Web interface to update the respective SSN users' contact details using the Central SSN Web interface (if the authority or a person reported also has an account in the SSN application).
When receiving information from EMSA MSS on the problems with contact points	B. NCA shall verify the information provided and update the Welcome on Board, if needed. The document shall later be sent to the EMSA/MSS. Additionally, the NCA shall update the respective SSN users' contacts using the SSN Web interface (if the authority or a person reported also has an account in the SSN application).
When requested for a yearly validation of the SSN lists by the EMSA MSS	C. NCA shall verify the list and update the 'Welcome on Board' document and send it to the EMSA/MSS. Additionally, the NCA shall update the respective SSN users' contacts using the SSN Web interface (if the authority or a person reported also has an account in the SSN application).

Time/When?	I.2. EMSA MSS
When receiving an updated list of contacts	A. EMSA MSS shall save the latest copy of the Welcome on Board document and update the internal lists used for the communication procedures 2.1, 2.10 (representatives, NCA 24/7, operational contacts or contractors).
When detecting a problem with contacts lists	B. EMSA MSS shall inform the relevant NCA on the problem with contact points (e.g. unavailability of the email, phone and fax) as detected during normal operations, reported by other SSN users or detected during distribution of information as per procedure 2.1
On a yearly basis	C. EMSA MSS shall send the Welcome on Board documents for validation to the NCAs.

2.7 Missing or mismatched information in SSN

What

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).

When

When a SSN data inconsistency is detected by EMSA MSS

When a SSN data inconsistency is detected by local users

Why

Directive 2002/59/EC, Art. 22a; IFCD Chapters 2.3; 4.6

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.

MSs should ensure that quality rules are applied at National level. The NCA 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.

Who

NCA being a focal point for all the quality related issues and for the report on the inconsistent or erroneous data.

LCA originator of the inconsistent or erroneous data.

EMSA MSS, which permanently monitors the data quality, the performance and the continuity of SafeSeaNet.

How

See specific Case I on the following pages.

Relation to other procedures

Communication procedure

(4.10)

Shall be put in place to ensure the proper identification/authentication between MSs or between MSs and EMSA MSS when using communication means such as phone or email.

Case I: SSN data inconsistency is detected by SSN users

Time/When?	**I.1. A SSN user detects missing, inconsistent or erroneous data**
When a SSN user detects missing, inconsistent or erroneous data	A. Its own NCA shall be contacted.

Time/When?	**I.2. NCA detecting missing, inconsistent or erroneous data**
When an NCA detects missing, inconsistent or erroneous data in SSN	A. NCA shall investigate the case and verify who was the actual provider of the missing, erroneous or inconsistent data.
When missing, inconsistent or erroneous data have been provided by National data providers	B. NCA shall contact the identified data provider and request the necessary resending or corrections. Alternatively, if possible, NCA can resend or correct data on its own. The NCA shall indicate in its communication whether the request is urgent or not. In case a request for correction is indicated as urgent (i.e. after an accident), the timeframe for providing the correct data is within 2 hours. In the other cases, the data can be provided within 48 hours.
When missing, inconsistent or erroneous data have been provided by other MS	C. NCA shall contact the MSS and report the case of missing, erroneous or inconsistent data requesting for further investigation and the relevant corrections. Additionally, NCA requestors can ask EMSA MSS to receive the missing information by any other appropriate means (e.g. if the latest AIS positioning report was missing, EMSA MSS may have access to other sources of information to obtain the relevant information).

Time/When?	**I.3. EMSA MSS**
When NCA reports an inconsistent, missing or erroneous data	A. EMSA MSS shall investigate the reported case and verify which Member State did not send the due information, or was the provider of the reported erroneous or inconsistent data.
When it is confirmed who provided the inconsistent data	B. EMSA MSS shall contact the identified NCA and request the necessary resending or corrections. The EMSA MSS shall indicate in its communication whether the request is urgent or not. In case of requests indicated as urgent (i.e. after an accident), the timeframe for providing the correct data is within 2 hours. In the other cases, the data can be provided within 48 hours.

Time/When?	**I.4. NCA originator of the inconsistent or erroneous data**
Once receiving report on missing, invalid or inconsistent data from MSS	A. NCA shall verify the information and send the due or corrected information to the SSN Central system. In case of requests indicated as urgent (i.e. after an accident), the timeframe for providing the data provided is within 2 hours. In other cases the data can be corrected within 48 hours.

2.8 Requesting and providing historical data and other types of data

What

The purpose of this procedure is to harmonise the method of requesting archived (historical) data from any data provider, and other data types (e.g. statistical) from the SSN system.

This procedure does not cover the requests for the data indicated as available via phone, fax or email (as per procedure 4.2).

When

When a Member State wishes to access data which is only available at the SSN Central Level (e.g. own-flagged ships' calls at another Member State's ports).

When a Member State wishes to access historical data which is unavailable at the SSN Central Level (e.g. for the investigation purposes).

When a Member State wishes to verify the quality and availability of the messages provided and requires a set of data for analysis.

When there are changes to the scope of the information provided to SSN (e.g. a Member State introduced additional authorities, messages, etc.) and the Member State concerned would like to compare data sets.

When a Member State wishes to obtain certain data following the tests.

Why

Directive 2002/59/EC, Art. 22a; IFCD v.1.0 Chapters 4.2; 5.2; 5.2.1

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.

It is important to ensure that information is provided to those users who have a need for the information and are granted with the proper access rights.

Who

Entitled SSN User requesting for SSN data

NCAs

EMSA MSS

How

See specific Case I on the following pages.

Relation to other procedures

Communication procedure

(4.10)

Shall be put in place to ensure the proper identification/authentication between Member States or between Member States and EMSA MSS when using communication means such as phone, fax or email.

Case I: Data is requested from the Central SSN or from National SSN systems

Time/When?	**I.1. SSN user requesting for data**
When SSN user requires specific data	A. Its own NCA shall be contacted and the template given below this procedure shall be used.
Following the positive assessment of the NCA	B. The foreseen time for obtaining data should not exceed 5 working days. User shall be aware that the NCA will verify the requestor access rights and will confirm whether the data is available on the National SSN level or whether it will be forwarded to another Member State via EMSA MSS.

Time/When?	**I.2. NCA**
Once receiving the request from a SSN user	A. NCA shall confirm the user's access rights (following the analysis of the template given below this procedure) and provide the requested data within 5 working days.
When data can be obtained only from SSN Central or from another MS	B. NCA shall forward the request to EMSA MSS.

Time/When?	**I.3. EMSA MSS**
When NCA requests for SSN data	A. Following the analysis of the request, EMSA MSS shall confirm whether the requested SSN data, stored at central level, has been provided by a Member State other than the requestor.
When requested SSN data has been provided by another Member State(s)	B. EMSA MSS is not entitled to provide the information from the Central SSN system unless authorised by the Member State(s) acting as data provider(s). Therefore, following a communication in writing, EMSA MSS must obtain authorization from the data provider(s).
When requested can be obtained only from another Member State SSN system	C. EMSA MSS shall forward the request to the relevant NCA.

Time/When?	**I.4. NCA of the Member State holding the data**
When NCA receives the request for specific SSN data	A. NCA shall provide the requested data within 5 working days following the reception of the request on the conditions that the relevant template for request is used.

Template

Requesting Authority details	**Contact Details:** **Phone:** **Fax:** **Email:** **Responsable Person:**
Requested data *(Historical, statistics, aggregated data, specific notifications, specific ports or ships etc.)* *Use the proposed fields as appropriate.*	**Specify**: (Free text) *Note 1: A requester may use further fields (below) to better specify the requested data criteria* **SSN Notification Type(s):** **Archived data:** **Other type (specify):**
Ship (s) identification or description *Note 2: Applicable only when the data requested is limited to a ship or a group of ships.*	**Identification:** **IMO:** **MMSI:** **Call Sign:** **Name:** **Description**:
Timeframe (if applicable)	**From:** **To:**
General Scope	**Quality or Quantity (amount):** **Availability:** **Communication link:**

Port identification or description
 	
Note 3: Applicable only when the data requested is limited to a port or a group of ports.
	Name(s):
	LOCODE(s):
	Port as: □ Last Port(s)/ □ Port(s) of Call/ □ Next Port(s)

Possible data providers	**NCA (Member State):**
	LCA (e.g. specific port)**):**

Area (if the coverage area can be defined by a polygon)	
Central SSN confirmation only *Note 4: EMSA MSS is not entitled to provide the information from the central SSN system unless authorised by the MS owning the data.*	**Additional permission of the actual data provider is needed? (To be filled by EMSA)** YES – which? NO
Preferable data carrier/ format	**Raw data/ Specific format** (specify):
Intended use of the information requested • *(e.g. investigation, inspection, infringement procedure, etc.)*	

Signature and stamp

2.9 Communication procedure

What The purpose of this procedure is to establish an identification/authentication method for data exchanged between two different Member States using communication means such as phone or email and to maintain the proper level of information security in the system and ensuring the proper monitoring of the access rights.

When When NCA enters in contact with EMSA MSS or another NCA on the SSN operational matters.

When SSN user enters in contact with NCAs.

When SSN user requests for information during a failure or an intervention.

When SSN user requests for information available via alternative communication means i.e. phone, fax and email.

Why Directive 2002/59/EC, Art. 22a; IFCD Chapters 3.1; 3.4; 7.2; 7.2.2.2; 7.2.2.5.

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

LCAs are free to exchange information directly, but only the procedure via NCAs as described here can guarantee the proper checking of access rights and a 24/7 response.

Who SSN Users requesting SSN data available via alternative communication means i.e. phone, fax and email or during maritime emergencies.

NCAs receiving or forwarding requests for SSN data available via alternative communication means i.e. phone, fax and email or during maritime emergencies.

EMSA MSS in the same manner as the above

How See specific Case I on the following pages.

Relation to other procedures

All procedures requiring direct contact and communication (2.1), (2.2), (2.5), (2.6), (2.7), (2.8), (2.10), (2.11)

Case I: When SSN user or an NCA of another Member State requests for SSN information (e.g. during a failure or an intervention) or when an SSN user submits any operational request for data to the NCA

Time/When?	I.1. SSN user
When requesting for information or submitting any operational request for data to the NCA	A. The SSN user shall contact its NCA and shall be ready to provide at least name, position, LOCODE, name of the service/office (LCA), phone, fax, to be authenticated by the NCA.
In case the NCA is not available	B. SSN user shall contact the EMSA/MSS forwarding his/her request, and shall be ready to provide information as indicated in I.1.A.

Time/When?	I.2. NCA
When national SSN user or another NCA requests for information or contacts for other operational matters	A. NCA shall authenticate the SSN User or the other Member State's NCA using the data provided (at least name, position, LOCODE, name of the service/office (LCA), phone, fax) and comparing it with the most recently updated SSN contacts list in the system (e.g. using SSN management console tool Authority Information Details/ User Information details functions) or following the national procedures.
When the authentication is successful	B. Actions described in the relevant procedures shall be executed maintaining the indicated timelines.
In case the authentication fails	C. NCA shall contact the EMSA MSS reporting the case of the failed authentication.

Time/When?	I.3. EMSA MSS
When national SSN user or another NCA requests for information	A. NCA shall authenticate the SSN User or the other Member State's NCA using the data provided (at least name, position, LOCODE, name of the service/office (LCA), phone, fax) and comparing it with the most recently updated SSN contacts list in the system. Note: In case of direct requests from users, which should be avoided, the MSS shall inquire why the NCA was not in position to support its SSN users.
When the authentication is successful	B. Actions described in the relevant procedures shall be executed maintaining the indicated timelines.
In case the authentication fails	C. EMSA MSS shall report the case and bring it to the attention of the SSN operation team of EMSA. This latter will assess the case and proposes the action considered necessary.

2.10 Central SafeSeaNet system switch to the Business Continuity Facility (BCF)

What The purpose of this procedure is: to increase the availability of SSN; to reduce the risk of a prolonged outage and; to allow a swift recovery in case of a major incident at EMSA in Lisbon.

When When the Central SSN switches to the BCF following a major incident at EMSA in Lisbon.

Why Directive 2002/59/EC, Art. 22a; IFCD Chapters 2.3; 4.1; 4.3; 4.4; 5.2; 5.3.

A BCF has been established to support the availability of the SSN system in case of a major failure of the Central SSN at EMSA premises.

Who NCA24/7 and EMSA MSS are responsible for implementing this procedure.

EMSA MSS system administrator and all SSN users should be aware of this procedure and the actions.

How See specific Case I on the following pages.

Relation to other procedures

Reporting technical failures or planned interventions (2.1) Shall be put in place to ensure that SSN users are properly informed on technical failures or planned interventions at Central or National SSN.

Back up communication procedure

(2.2) Shall be put in place to make sure that data is available by alternative means of communication once the system is unavailable.

Communication procedure

(2.10) Shall be put in place to ensure the proper identification/authentication between Member States or between Member States and EMSA MSS when using communication means such as phone, fax or email.

Case I: When central SSN switches to the BCF following a major issue at EMSA premises

Time/When?	I.1. EMSA MSS
Within 2 hours after the switch	A. EMSA MSS notifies NCA24/7 that Central SSN switched to BCF.
When the connection between BCF and national SSN system is established	B. EMSA SSN shall monitor that the national SSN systems provide all required information.
If a failure in the BCF or in the national SSN system is detected	C. Procedure 2.1 “reporting technical failure or planned intervention” shall be applied.

Time/When?	I.2. NCA
When receiving the notification from EMSA/MSS that central SSN switches to BCF	A. If the national SSN system is not BCF ready: ensure that the national SSN system points to BCF (e.g. by manual IP switch). SSN web interface might be used as a back-up solution for reporting. Back-up procedures should also be executed at national level. S-TESTA users shall continue pointing to EMSA which will redirect the connection to BCF using internet. If the national SSN system is BCF ready then the connection should be enforced automatically.
When the connection is established between the national SSN and the BCF	B. Verify whether all the mandatory information required by Directive 2002/59/EC is provided to the Central SSN and whether details are available upon request (national tools or the SSN web interface can support such verifications).
When a failure in the provision of the mandatory information is detected	C. Procedure 2.1 “reporting technical failure or planned intervention” shall be applied

2.11 Failover of a National SSN system or a National AIS system or Regional AIS server

What The purpose of this procedure is: to increase the availability of the national SSN or a National AIS system or Regional AIS server; to reduce the risk of a prolonged outage and; to allow a swift recovery in case of a major incident at national level.

When When a failover process takes place following a major incident affect the National SSN or the National AIS system or Regional AIS server.

Why Directive 2002/59/EC, Art. 22a; IFCD Chapters 2.3; 4.1; 4.3; 4.4; 5.2; 5.3.

Failover is a process to support the availability of the SSN system or National AIS system or Regional AIS server. This is an automatic process usually operating without a warning. Some systems require human intervention to failover.

Who NCA24/7, the RS 24/7 and EMSA MSS are responsible for implementing this procedure.

EMSA MSS system administrator and all SSN users should be aware of this procedure and the actions.

How See specific Case I on the following pages.

Relation to other procedures

Reporting technical failures or planned interventions (2.1) Shall be put in place to ensure that SSN users are properly informed on technical failures or planned interventions at Central or National SSN.

Back up communication procedure (2.2) Shall be put in place to make sure that data is available by alternative means of communication once the system is unavailable

Communication procedure (2.10) Shall be put in place to ensure the proper identification/authentication between Member States or between Member States and EMSA MSS when using communication means such as phone or email.

Case I: When the failover process for a National/Regional system initiates

Time/When?		I.1. NCA/Regional AIS server
Within 2 hours after the failover	A.	The NCA24/7 or the Regional AIS server 24/7 sends a notification to EMSA MSS about the failover of a national/regional system.
If EMSA MSS reports that data are missing or communication failed with the national/regional system	B.	Procedure 4.1 “reporting technical failure or planned intervention” shall be applied

Time/When?		I.2. EMSA MSS
Within 2 hours from the reception of the notification of a National / Regional system failover	A.	EMSA MSS analyses the data provided by the reporting MS/Regional AIS server and carries out a situation analysis.
If it is detected that data are missing or the communication failed with the national/regional system	B.	Procedure 2.1 “reporting technical failure or planned intervention” shall be applied.

2.12 National AIS data delivery back-up procedure

What

The purpose of this procedure is to:

- reduce the risk of loss of ship position data (AIS data) during failures or scheduled interruptions affecting national AIS systems[7] or their connections with regional AIS servers (RS) and/or the central SSN system.
- increase the availability of national AIS systems to provide AIS data to the central SSN (through the regional AIS server or directly).

When

The national AIS system is not providing ship AIS positions to SSN. Two possible cases are envisaged:

- Scheduled interruption and/or failure (affecting the national AIS system or its connection with the RS or central SSN system) which lasts less than 12 hours.
- Failure (affecting the national AIS system or its connection with the RS or central SSN) which lasts more than 12 hours.

Who

The SSN National Competent Authorities (NCAs), Regional AIS Servers (RSs) and EMSA/MSS are responsible for implementing this procedure.

Why

Directive 2002/59/EC (Annex 2.3) gives reference to the Interface and Functionalities Control Document (IFCD).

According to Chapter 2.3 of the IFCD, SSN supports the exchange of AIS position information.

According to Chapter 2.5.3 of the IFCD, SSN is equipped with a streaming mechanism which enables the near-real time exchange of ship positions obtained via the AIS networks, supporting national SSN systems to provide AIS information to regional AIS servers and/or the central SSN system.

According to Chapter 4.3 of the IFCD, the SSN systems (Central and National) shall be maintained at a minimum of 99% over a period of one year, with a maximum permissible period of interruption of 12 hours.

According to Chapter 4.4 of the IFCD, in the event of a failure or a scheduled 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).

How

See specific Cases I, II, III in the following sections.

[7] National AIS system is part of the national SSN system relying AIS data to the central SSN (through regional AIS server or directly). National AIS system also includes the NPR (national proxy software delivered by regional AIS server) or SSN PA (SSN Proxy Application software delivered by EMSA) and hosted by Member States.

Relation to other procedures

- Procedure 2.1 - Reporting technical failures or interventions: shall be maintained to ensure that SSN users are properly informed on technical failures or planned interventions at the central and national SSN levels.

- Procedure 2.12 - Failover of a National SSN system or a National AIS system or Regional AIS server

Case I: A failure (incident) or planned intervention in the national AIS system affecting the collection and/or processing of AIS data (i.e. malfunctioning of the national AIS server/system)

Time/When?	I.1. NCA
A failure is detected or an intervention is planned/required in the national AIS system	The National Competent Authority (NCA) shall execute the actions described in procedure 2.1 to inform SSN users. The NCA shall inform RS by e-mail. In the case of an incident, the NCA shall inform the RS / EMSA MSS[8] about the failure and the recovery actions needed/taken so far.
As soon as possible	The NCA may establish/introduce temporary procedures to provide data or to switch national AIS system to the business continuity facility.
Incident/intervention closed	The NCA shall execute the actions described in procedure 2.1 to inform SSN users. The NCA shall inform the RS by e-mail.
Within 12 hours after the recovery from a failure of the national AIS system	In the case of an incident, the NCA shall submit a detailed report describing the failure that occurred, the timeframe and the recovery actions taken, informing: • MSS (if its data for the central SSN are provided directly through the SSN PA connection), or; • RS (if its data for the central SSN system are provided through the RS NPR[9]).

Time/When?	I.2. AIS Regional Server (RS)
A failure is detected	In cases where the incident is detected by the RS staff: - The EMSA MSS shall be informed and the incident time[10] shall be registered. - The RS shall set the priority level.
As soon as possible	In the case of an incident, the RS shall inform the source Country in accordance with the regional agreement in force. If the source Country does not react, the RS shall inform the EMSA MSS.
Within the incident analysis period (analysis time as in SLA)	Investigation and diagnosis The RS 24/7 shall assess whether all of the RS systems (including the SSN PA) are functioning as expected. A free form report is sent by email to EMSA MSS, informing if the observed

[8] Depending on the solution maintained (i.e .the data submission via NPR or SSN PA).

[9] NPR: National Proxy Application provided by AIS Regional Servers and hosted by National AIS System

[10] Date-time group should be used to register the incident time.

	failure was caused by the AIS system of the participating State. The RS shall provide an assessment of the potential root cause of the incident.
During the incident/planned intervention	The RS shall monitor the affected connection (if connected through the NPR).
Incident/intervention closed	The RS shall inform the MSS by e-mail that all connections are operational.
The next working day after the incident (12:00 UTC at the latest).	A detailed report of the AIS data delivery incident shall be sent by email to the EMSA MSS

Time/When?	**I.3. EMSA MSS**
A failure is detected	In cases where the incident is detected by MSS staff: • The incident time shall be registered. • The MSS shall set the priority level.
As soon as possible	In the case of an incident, the MSS shall launch procedure “SSN-IMG-001 Incident Management on National SSN” The EMSA MSS shall inform the SSN NCA 24/7 of the national system affected and the RS[11] - when the incident is detected. The acknowledgment time shall be registered.
During the incident	The MSS shall monitor the affected connection (if connected through the SSN PA[12]).
Incident closed	The incident closure time shall be registered when the national system has recovered and become operational - as soon as confirmation is received from the concerned parties (the affected country and/or the RS) or the MSS monitoring.

[11] Depending on the solution maintained (i.e. if its data for the central SSN are provided via NPR).

[12] PA: SSN proxy Application provided by EMSA and hosted by National AIS system in case of directed connection for the provision of AIS

Case II: A failure (incident) or planned intervention affecting the connection of national AIS system with the AIS regional server (RS) or central SSN system13 (i.e. the communication network failure or the NPR/ SSN PA connection to the RS/ central SSN failure)

Time/When?	II.1. NCA
A failure is detected or an intervention is planned/required in the national AIS system	The National Competent Authority (NCA) shall execute the actions described in procedure 2.1 to inform SSN users. In the case of an incident, the National Competent Authority (NCA) shall inform the RS / MSS about the failure and the recovery actions needed/taken so far[14].
As soon as possible	The NCA may establish/introduce temporary procedures to provide data, or to switch the national AIS system to the business continuity facility.
Within the timeframe of 12 hours from the beginning of the detected failure/ scheduled intervention	The NCA shall ensure that AIS data are buffered[15] allowing their retransmission (either automatically or manually) to RS /central SSN once the connection between national AIS system and the RS/ central SSN has been recovered[16]. If data buffering is not available, the NCA shall ensure that AIS data are stored, allowing their retransmission (either automatically or manually) to RS /central SSN once the connection between national AIS system and the RS /central SSN has been recovered[17].
When the detected failure/ scheduled intervention lasts more than 12 hours from the beginning of a detected failure/ started intervention.	The NCA shall ensure that AIS data are stored, allowing their retransmission (either automatically or manually) to RS/central SSN once the connection between national AIS system and the RS /central SSN has been recovered[18]. Data down-sampling can be applied (e.g. up to 1 position per vessel/hour) when re-sending messages for up to 2 weeks.
Incident/intervention closed	The NCA shall execute the actions in procedure 2.1 to inform SSN users. The NCA shall inform the RS/MSS by e-mail[19].
Within 12 hours after the recovery from a failure/ intervention.	In the case of an incident, the NCA shall submit a detailed report describing the failure that occurred, the timeframe and the recovery actions taken, to: a) the EMSA MSS - if the data are provided directly to the SSN system (through the SSN PA connection), or; b) the RS - if the data are provided to the SSN system through the RS NPR.
Within 24 hours after the recovery from a	The SSN NCA shall ensure that the data buffered/stored during the outage of the transmission have been retransmitted to the RS/central SSN system

[13] Depending on the connection maintained (i.e. data submission via NPR or SSN PA).

[14] See footnote Nr.13

[15] A data buffering is a temporarily holding of data while it is being moved from one place to another. A buffer contains data that is stored for a short amount of time. The NPRs delivered by the RSs and hosted by the MSs have a limited buffering capability (for appr. 12 hours, depending the data size).

[16] See footnote Nr.13

[17] See footnote Nr.13

[18] See footnote Nr. 13

[19] See footnote Nr.13

failure/intervention.	(depending on the connection maintained). If the stored/buffered data cannot be retransmitted, the NCA shall provide these data via alternative means (e.g. e-mail, the NPR/SSN PA backlog, FTP etc.). The data retransmission/delivery shall be agreed and coordinated with the RS/MSS (depending on the connection maintained).

Time/When?	**II.2. Regional Server**
A failure is detected	In cases where the incident is detected by the RS staff: - The EMSA MSS shall be informed and the incident and acknowledgement time shall be registered. - The RS shall set the priority level.
As soon as possible	In the case of an incident, the RS shall inform the source Country in accordance with the regional agreement in force. If the source Country does not react, the RS shall inform MSS.
Within the incident analysis period (analysis time as in the SLA)	Investigation and diagnosis. The RS 24/7 shall assess whether all of the RS systems (including the SSN PA) are functioning as expected. A free form report is sent by email to EMSA MSS informing if the failure was caused by the AIS system of the participating State. The RS shall provide an assessment of the potential root cause of the incident.
During the incident	The RS shall monitor the affected connection (if connected through the NPR). In the case of the NPR connection to the RS failure the RS shall provide the required assistance to the affected MS in accordance with the regional agreement in force (e.g. the connection's testing) (if requested).
Incident/intervention closed	The RS shall inform MSS by e-mail that all connections are operational and launch the procedure to receive the buffered/stored data from the affected MS (when needed).
The next working day after the incident (12:00 UTC at the latest).	A detailed report of the AIS data delivery incident is sent by email to the EMSA MSS

Time/When?	**II.2. EMSA MSS**
A failure is detected	In cases where the incident is detected by the MSS staff:

	• The incident time shall be registered. • The MSS shall set the priority level.
As soon as possible	In the case of incident, the MSS shall launch the procedure “SSN-IMG-001 Incident Management on National SSN” The EMSA MSS shall inform the SSN NCA 24/7 of the national system affected and the RS[20] - when the incident is detected. The acknowledgment time shall be registered;
During the incident	The MSS shall monitor the affected connection (if connected through the SSN PA). In the case of the SSN PA connection’s to the central SSN failure the MSS shall provide the required assistance to the affected MS in accordance with the agreement/procedures in force (e.g. the connection’s testing) (if requested).
Incident closed	The incident closure time shall be registered when the connection of national system has recovered and become operational - as soon as confirmation is received from the concerned parties (the affected country and/or the RS) or the MSS monitoring.

[20] Depending on the connection maintained (i.e. data submission via NPR or SSN PA).

Case III: A failure (incident) or planned intervention affecting the national AIS server's connection with NPR or SSN PA, or the NPR/SSN PA failure

Time/When?	III.1. NCA
An NPR/SSN PA failure has been detected or an intervention is planned/required at the national AIS system	The National Competent Authority (NCA) shall execute the actions described in procedure 2.1 to inform SSN users. In the case of an incident, the NCA shall inform the RS/ MSS[21] about the failure and the recovery actions needed/taken so far.
As soon as possible	The NCA may establish/introduce temporary procedures to provide data or to switch the national AIS system to the business continuity facility.
During the incident/ scheduled intervention	The NCA shall ensure that AIS data are buffered by national AIS system, allowing their retransmission (either automatically or manually) to RS/central SSN once the connection between the national AIS system/server and the NPR/SSN PA has been recovered or the NPR/ SSN PA failure has been solved[22]. If data buffering is not available, the NCA shall ensure that AIS data are stored, allowing their retransmission (either automatically or manually) to RS/central SSN once the connection between the national AIS system/server and the NPR/ SSN PA has been recovered or the NPR/SSN PA failure has been solved[23].
Incident/intervention closed	The NCA shall execute the actions described in procedure 2.1 to inform SSN users. The NCA shall inform the RS/MSS by e-mail[24].
Within 12 hours after the recovery from a failure/ intervention.	In the case of an incident, the NCA shall submit a detailed report describing the failure that occurred, the timeframe and the recovery actions taken, to: a) MSS - if the data is provided to the central SSN system through the SSN PA connection), or; b) RS - if the data is provided to the central SSN system via the NPR.
Within 24 hours after the recovery from a failure/intervention.	The SSN NCA shall ensure that the data buffered/stored during the outage of the transmission are retransmitted to the RS/ central SSN (depending on the connection's solution maintained). If the data cannot be retransmitted, the NCA shall provide the stored/buffered data via alternative means (e.g. email, SSN PA/ NPR backlog, FTP etc.). The data retransmission/delivery shall be agreed and coordinated with the

[21] Depending the solution applied for the data transmission to SSN. See also footnote 8.
[22] See footnote 8
[23] See footnote 8
[24] See footnote 8

	RS/MSS (depending on the connection’s solution maintained). Data down-sampling can be applied (e.g. up to 1 position per vessel/hour) when re-sending messages for up to 2 weeks.

Time/When?	III.2. AIS Regional Server (RS)
An NPR failure is detected	In cases where the incident has been detected by the RS staff: - The EMSA MSS shall be informed and the incident and acknowledgement time shall be registered. - The RS shall set the priority level.
As soon as possible	In the case of an incident, the RS shall inform the source Country in accordance with the regional agreement in force. If the source Country does not react, the RS shall inform the MSS.
Within the incident analysis period (the analysis time as in the SLA)	Investigation and diagnosis. The RS 24/7 shall assess whether all of the RS systems (including the SSN PA) are functioning as expected. A free form report is sent by email to EMSA MSS informing if the observed failure was caused by AIS system of the participating State. The RS shall provide an assessment of the potential root cause of the incident.
During the incident	The RS shall monitor the affected connection (if connected through the NPR). In the case of the NPR failure, the RS shall provide the required assistance to the affected MS in accordance with the regional agreement in force (e.g. the NPR testing etc.).
Incident/intervention closed	The RS shall inform MSS by e-mail that all connections are operational and launch the procedure for receiving the buffered/stored data from the affected MS (when needed).
The next working day after the incident (12:00 UTC at the latest).	A detailed report of the AIS data delivery incident is sent by email to the EMSA MSS

Time/When?	III.3. EMSA MSS
A failure is detected	In cases where the incident is detected by the MSS staff: • The incident time shall be registered.

- The MSS shall set the priority level.

As soon as possible

In the case of an incident, the MSS shall launch the procedure “SSN-IMG-001 Incident Management on National SSN”

The EMSA MSS shall inform the SSN NCA 24/7 of the national system affected and the RS[25] - when the incident has been detected. The acknowledgment time shall be registered;

During the incident

The MSS shall monitor the affected connection (if connected through the SSN PA).

In the case of the SSN PA connection’s to the central SSN failure the MSS shall provide the required assistance to the affected MS in accordance with the agreement/procedures in force (e.g. the SSN PA testing) (if requested).

Incident closed

The incident closure time shall be registered when the connection of national system has recovered and became operational - as soon as confirmation is received from the concerned parties (the affected country and/or the RS) or the MSS monitoring.

[2525] Depending on the connection maintained (i.e. data submission via NPR or SSN PA)

European Maritime Safety Agency
Praça Europa 4
1249-206 Lisbon, Portugal
Tel +351 21 1209 200
Fax +351 21 1209 210
emsa.europa.eu

EMSA