SIOFA | APSOI
Southern Indian Ocean Fisheries Agreement
Accord relatif aux Pêches dans le Sud de l'Océan Indien

2nd Meeting of the SIOFA VMS Working Group (VMSWG-02)

Online, 29th February 2024

VMSWG-02-03

Proposed Data Confidentiality and Security Measures

SIOFA Secretariat

Document Type	working paper ✔ information paper ☐
Distribution	Public ✔ Restricted [1] ☐ Closed session document [2] ☐

Abstract

One of the SIOFA VMSWG mandates was to propose Data Confidentiality and Security Provisions for the SIOFA VMS. At the 1st Meeting of the SIOFA WG, it was agreed that the Secretariat would propose a section in the SIOFA VMS SSPs for data confidentiality and security. While these have been included in the second draft of the SSPs, the Secretariat noted that the inclusion of these provisions in a new section of the SSPs it may create some disparity in its implementation as some of these provisions are largely covered by CMM 16 (2023) (Vessel Monitoring System), recalling that the CMM is binding, while the SSPs have been redrafted to be non-binding. As such, the secretariat has found it necessary to propose other alternative modalities to implement the data confidentiality and security provisions.

Recommendations (for proposals and working papers only)

- the VMS WG02 reviews and provides guidance on what would be the best modality to implement the data confidentiality and security measures.

[1] Restricted documents may contain confidential information. Please do not distribute restricted documents in any form without the explicit permission of the SIOFA Secretariat and the data owner(s)/provider(s).
[2] Documents available only to members invited to closed sessions.

Introduction

At the 1st Meeting of the SIOFA WG, it was agreed that the Secretariat would propose a section in the SIOFA VMS SSPs for data confidentiality and security. While these have been included in the second draft of the SSPs, the Secretariat noted that the inclusion of these provisions in a new section of the SSPs it may create some disparity in its implementation as some of these provisions are largely covered by *Conservation and Management Measure for the establishment of a SIOFA Vessel Monitoring System (Vessel Monitoring System) (CMM 16(2023)),* recalling that the CMM is binding, while the SSPs have been redrafted to be non-binding. As such, the secretariat has found it necessary to propose other alternative modalities to implement the data confidentiality and security provisions.

Overview of Key Confidentiality and Security Provisions in Other RFMOs

The Secretariat conducted an analysis of data confidentiality and security for regional VMS systems in other Regional Fisheries Management Organizations (RFMOs), and the Commission for the Conservation of Antarctic Marine Living Resources (CCAMLR) and the key measures noted were the following:

- General Provisions
  - Requirement to comply with Confidentiality and Security Provisions
  - Requirement to inform MoP on measures taken to comply with confidentiality and Security Provisions
  - Requirement for CCPs and Secretariat to utilize data pursuant to CMM 16
- Confidentiality Measures
  - Classification of VMS Data as "Confidential Data"
  - Nomination of VMS Contact Point for request of VMS Data
  - Procedures for request of VMS Data
  - Criteria for data release
  - Requirement to delete VMS data once it has served its purpose, and confirm deletion in writing to secretariat.
  - Requirement to make VMS data for HSBI, SAR and Surveillance to inspectors and other designated officials only
  - Time period prior to operation whereby CCPs can make requests for VMS Data
- Security Measures
  - Requirement to ensure secure treatment of VMS data
  - Requirement to implement appropriate technical and organizational measures to protect VMS data against accidental or unlawful destruction, loss alteration, unauthorized disclosure or access, and against all inappropriate form of processing.
  - Requirement for Secretariat to publish list of "VMS Points of Contacts"
  - Requirement for VMS data to be transferred using secure protocols
  - System Access Controls
  - Authenticity and data access control
  - Communication Security
  - Data Security
  - Security Procedures

Table 1 of Annex 1 of this document includes a more detailed overview of these measures.

These provisions were implemented in various ways, but the most common approach was as an annex to the main implementing instrument. It most cases observed, these provisions were binding.

Implementing Data Confidentiality and Security Measures in the SIOFA Context

As agreed by the 10th Meeting of the Parties, the SIOFA VMS WG has been tasked, among other things, to define Data Confidentiality and Security measures. During its 1st Meeting, the VMS WG proposed that these measures are included as a section of the VMS SSPs.

To accomplish this, the Secretariat has taken most of the key measures and included them in a new section of the SSPs in the second draft of the SSPs (Paper WMSWG-02-02), being mindful that number of those measures have already been provided for by CMM 16 (2023)., and to some extent, they are also present in *Conservation and Management Measure for Data Confidentiality and Procedures for access and use of data (Data Confidentiality)* (CMM 03(2016)). However, with the SSPs now potentially being a non-binding instrument, this may create disparity in how these measures are implemented and applied.

As such, this paper proposes an alternate modality to implement these measures, by incorporating the Data Confidentiality and Security Measures within these two CMMs, i.e. CMM 16 (2023) and CMM 03 (2016). The amendments to these two CMMs are also presented in Annex 1 of this document, with the amended CMMs in Annex 2 and Annex 3 for CMM 03 (2016) and CMM 16 (2023), respectively.

Conclusion

To conclude, the VMSWG02 are welcome to assess these proposals against the inclusion of the data confidentiality and security measures within the potentially non-binding SSPs.

Annex 1: Key Elements of data Confidentiality and Security Provisions in RFMO VMS

Classification	Element	Applicability	CMM 03	CMM 16	Annex to CMM 16 [New Section in SSP]	Remarks	Proposed Amendment to CMM 03 […for Data Confidentiality, Security Measures, and Procedures…]	Proposed Amendment to CMM 16
General Provisions	*Requirement to comply with Confidentiality and Security Provisions*	*Secretariat, CCPs*		Para 31		Para 31 of CMM 16 may be construed as not requiring compliance with security measures but requiring the secure and confidential treatment of VMS data.	1 bis. CCPs and the Secretariat shall take necessary measures to comply with these confidentiality and security measures.	32 bis. (or 31 ext.) CCPs and the Secretariat shall take necessary measures to comply with the agreed confidentiality and security provisions for the SIOFA VMS, [including applicable provisions under CMM 03.]
	Requirement to inform MoP on measures taken to comply with confidentiality and Security Provisions	*Secretariat*	x	x	x	None	The Secretariat shall inform the MoP, on measures taken to implement the[se] confidentiality and Security requirement/measures/provisions.	35. …including measures taken to implement the confidentiality and Security requirements/measures/provisions.
	Requirement for CCPs and Secretariat to utilize data pursuant to CMM 16	*Secretariat, CCPs*		x	x	None		32 ter. The CCPs and the Secretariat shall only use VMS data for the purposes specified in this CMM.
Confidentiality	*Classification of VMS Data as "Confidential Data"*	*Secretariat, CCPs*	Para 2 e-i	Para 31		"Effort" data in CMM 03 may also include VMS data. As such all provisions related to finer level effort data may also be applicable to VMS data. CMM 03 may be amended to improve clarity (remove potential ambiguity) Para 31 in CMM 16 may also need amendment to explicitly include ALC details as confidential data. Note para 13 of CMM 10 (2023)	See proposed amendment to Para 2 e)	31. All CCPs, the Secretariat, the SIOFA Scientific Committee and its subsidiary bodies, and any SIOFA VMS provider shall ensure the secure and confidential treatment of VMS data, including ALC details in their respective electronic data processing facilities, in particular where the processing involves transmission over a network.
	Nomination of VMS Contact Point for request of VMS Data	*CCPs*		Para 11		None		
	Procedures for request of VMS Data		x	Paras 22 - 29	x	Does not require Secretariat to make data available to a secure email specified at the time of request.	2. j) (new sub paragraph) The Secretariat shall only provide confidential data to a secure email address specified at the time of making a request for data.	22. ...The Secretariat shall only provide VMS data to a secure email address specified at the time of making a request for data.
	Criteria for data release	*Secretariat, CCPs*	x	x	x	CMM provides for the release of VMS data for SAR, HSBI and Surveillance Missions without the consent of the flag CPP. It also provides for other uses (which is undefined and unrestricted), including for the scientific committee, subject to the consent of the flag CCP. There are no set criteria for the release of such data and how these data may be used, which is commonly practised in other RFMOs. (e.g. catch documentation schemes etc). (Para 22 and 28 implies no restriction to use of requested VMS data)		To seek guidance from the WG as to when CCPs can make request for VMS Data, outside of para 23 and the SC.

	Requirement to delete VMS data once it has served its purpose, and confirm deletion in writing to secretariat.	*CCPs*		**Para 24, 28**	**x**	CMM requires deletion of VMS data received pursuant to para 24 only. No provision requiring receiving CCPs to delete VMS data once it has served its purpose, in any other cases.		28. …CCPs shall destroy/delete requested VMS data, once the data has served its intended purpose, and confirm their deletion to the secretariat in writing, without delay.
	Requirement to make VMS data for HSBI, SAR and Surveillance to inspectors and other designated officials only	*CCPs*		**Para 24 b**		None		
	Time period prior to operation whereby CCPs can make requests for VMS Data	*CCPs*		**Para 25**		None		
	Requirement to ensure secure treatment of VMS data	*Secretariat, CCPs*		**Para 31**		None		
	Requirement to implement appropriate technical and organizational measures to protect VMS data against accidental or unlawful destruction, loss alteration, unauthorized disclosure or access, and against all inappropriate form of processing.	*Secretariat, CCPs*	**x**	**x**	**x**		3 Procedures for safeguarding [and securing] records, and databases, and [VMS data] will be as follows: d) (new sub paragraph) CCPs and the Secretariat shall take appropriate measures to protect all data against accidental or unlawful destruction, loss alteration, unauthorised disclosure or access, and against all inappropriate forms of processing.	31. …CCPs and the Secretariat shall take appropriate measures to protect VMS data against accidental or unlawful destruction, loss alteration, unauthorized disclosure or access, and against all inappropriate form of processing.
	Requirement for Secretariat to publish list of "VMS Points of Contacts"	*Secretariat*		**Para 11**		None		
	Requirement for VMS data to be transferred using secure protocols	*Secretariat, CCPs*		**SSPs**		None		
Security (propose new section under CMM 03)	*System Access Controls*	*Secretariat*	**x**		**x**	None	***New Section in CMM 03*** The following security measures shall be mandatory for the SIOFA VMS: System Access Control: the system has to withstand break-in attempts from unauthorised persons Authenticity and data access control: the system has to be able to limit access of unauthorized parties to only the data necessary for their task, via a flexible user identification and password mechanism -VMS data must be securely communicated; communication	
	Authenticity and data access control	*Secretariat*	**x**		**x**	None		

	Communication Security	*Secretariat*	x		x	None	communicated. communication between CCPs, Service Provider and the Secretariat shall use secure protocols, in accordance to with the VMS Specifications, Standards and Procedures (SSPs). -Data Security: all vms data received by the Secretariat shall be securely stored for a predetermined time, and shall not be tampered with -Security Procedures: Secretariat shall implement the Information System Security Policy to ensure roper access to the system, (hardware and software) system administration and maintenance, backup and general usage of the system.	
	Data Security	*Secretariat*	x		x	None		
	Security Procedures	Secretariat	x		x	None		

Formatted: English (United States)

CMM 16(2023)[1]

Conservation and Management Measure for the establishment of a SIOFA Vessel Monitoring System (Vessel Monitoring System)

The Meeting of the Parties to the Southern Indian Ocean Fisheries Agreement:

RECALLING Article 6(1)(h) of the Southern Indian Ocean Fisheries Agreement (SIOFA) which requires the Meeting of the Parties to develop rules and procedures for the monitoring, control and surveillance of fishing activities in order to ensure compliance with conservation and management measures adopted by the Meeting of the Parties including, where appropriate, a system of verification incorporating vessel monitoring and observation of vessels operating in the Agreement Area;

MINDFUL of Article 18(3) of the Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks (UNFSA) which outlines the duties of the flag State, including to take measures to ensure recording and timely reporting of vessel position, catch of target and non-target species, fishing effort and other relevant fisheries data, and to ensure the monitoring, control and surveillance of vessels, their fishing operations and related activities by, inter alia, the development and implementation of vessel monitoring systems;

FURTHER MINDFUL of the importance of international cooperation in the fight against illegal, unreported and unregulated (IUU) fishing, in particular through the exchange of information and effective monitoring, control and surveillance;

RECALLING paragraph 14 of the SIOFA Conservation and management measure for the Monitoring of Fisheries in the Agreement Area (CMM 10(2023)) to develop specifications and propose rules and procedures for the establishment of a SIOFA Vessel Monitoring System;

MINDFUL of the key principles upon which the vessel monitoring system should be based, including the confidentiality and security of information handled by the system, and its efficiency, cost-effectiveness and flexibility;

***ADOPTS* the following Conservation and Management Measure (CMM) in accordance with Articles 4 and 6 of the Agreement:**

Definitions

1. The following definitions shall apply to this CMM:
   a) "Automatic location communicator" (ALC) means a satellite-based on-board device that is capable of continuously, automatically and independently of any intervention of the vessel, transmitting VMS position reports;
   b) "Fisheries monitoring centre" (FMC) means the authority or agency of a Flag CCP responsible for managing the VMS for its flagged fishing vessels;
   c) "Vessel Monitoring System" (VMS) means a satellite-based monitoring system which, at regular intervals, provides VMS position reports;
   d) "SIOFA VMS" means the SIOFA Vessel Monitoring System established under this CMM;
   e) "Manual reporting" means the transmission via alternative means of the position reporting of a fishing vessel when an ALC fails to transmit VMS position reports;
   f) VMS position reports shall include at least the following data:
      i. the fishing vessel's unique vessel identifier;

[1] Several paragraph references have been corrected in January 2024.

ii. the current geographical position (latitude and longitude) of the vessel;
iii. the date and time (UTC) of the fixing of the position of the vessel;
iv. the vessel's speed; and
v. the vessel's course.

Objective

2. The main objective of the SIOFA VMS is to monitor in an automatic, continuous and cost-effective manner the movements and activity of fishing vessels operating in the Agreement Area to ensure compliance with SIOFA CMMs.

Application

3. The SIOFA VMS shall apply to all fishing vessels flying the flag of a Contracting Party, cooperating non-Contracting Party or participating fishing entity (CCP) that are entered onto the SIOFA Record of Authorised Vessels and operating in the Agreement Area, as defined in Article 3 of the Agreement.

Nature and specifications of the SIOFA VMS

4. The SIOFA VMS shall be administered by the SIOFA Secretariat under the guidance of the Meeting of the Parties.

5. Each CCP shall ensure that all fishing vessels flying their flag entered onto the SIOFA Record of Authorised Vessels and operating in the Agreement Area are fitted with an operational ALC that complies with the minimum standards for ALCs described in Annex 1.

6. Each CCP shall ensure that all fishing vessels flying their flag referred to in paragraph 3 report VMS position reports automatically while they are operating in the Agreement Area either:

    a) to the Secretariat via their FMC; or

    b) simultaneously to both the Secretariat and their FMC.

7. CCPs that choose to report under option (a) of paragraph 6 shall automatically forward VMS position reports to the Secretariat without delay but not later than one hour after receipt.

8. CCPS shall ensure that VMS position reports are reported automatically[2] by each of their vessels while operating in the Agreement Area:

    a) at least once every hour as provided for in paragraph 25 of CMM 15(2023) (Management of Demersal Stocks), and;

    b) at least once every two hours in other circumstances.

9. The Meeting of the Parties shall establish VMS position report format and transmission standards, specifications and procedures prior to the entry into operation of the SIOFA VMS.

[2] In the event that the connection between the ALC and the satellite is temporarily unavailable, the data referred to in paragraph 1(f) of this Measure shall still be collected but shall instead be transmitted as soon as the satellite connection becomes available again.

10. Each CCP shall ensure that their FMC can automatically receive and, for those CCPs whose vessels transmit VMS position reports in accordance with paragraph 6 a), transmit VMS position reports from ALCs. Each CCP shall provide backup and recovery procedures in case of system failures.

11. Each CCP shall provide the Secretariat with the name, address, email, and telephone numbers of the relevant authorities of its FMC and shall designate a VMS Point of Contact for the purposes of any communication regarding the SIOFA VMS ("VMS Point of Contact"). Each CCP shall notify the Secretariat of any changes to these details within 30 days after such changes take effect and the Secretariat shall promptly notify this information to the other CCPs and make it available on the non-public area of the SIOFA website.

12. Each CCP shall ensure that in vessels flying their flag:
    a) the ALC is not tampered with in any way;
    b) VMS position reports are not altered in any way;
    c) the antenna or antennae are connected to the ALC and not obstructed in any way;
    d) the power supply of the ALC is not interrupted in any way;
    e) the ALC is not removed from the vessel except for the purpose set out in paragraph 15; and
    f) The satellite navigation decoder and transmitter shall be fully integrated and housed in the same tamper-proof physical enclosure.

Procedure for manual reporting

13. In the event of non-reception of four consecutive, expected programmed VMS positions, the Secretariat shall notify the CCP whose flag the vessel is flying. The Flag CCP shall immediately notify the vessel Master and direct the Master to provide it with manual reports every four hours of the vessel's position in accordance with the reporting frequency under paragraph 8. The Flag CCP shall ensure that this manual reporting is transmitted to the Secretariat, either by the flag CCP or by the fishing vessel, with a clear distinction between reports that are manual and those that are automatic.

14. The Flag CCP shall ensure that the manual reports include at least the information referred to in paragraph 1(f)(i), (ii) and (iii). If automatic reporting to the SIOFA VMS has not been re-established within 60 days of the commencement of manual reporting, the Flag CCP shall order the vessel to cease fishing, stow all fishing gear and return immediately to port in order to undertake repairs or replacement.

15. Following a technical failure or non-functioning of the ALC, the Flag CCP shall ensure that the fishing vessel only leaves port once the ALC fitted on board is fully functioning to the satisfaction of the competent authorities of the Flag CCP. By derogation, the Flag CCP may authorise the fishing vessel to leave port with a non-functioning satellite-tracking device for its repair or replacement.

16. The Flag CCP shall ensure that the vessel recommences fishing in the Agreement Area only when the ALC has been confirmed as operational by its FMC. Four consecutive,

programmed VMS positions must have been received by the FMC to confirm that the ALC is fully operational.

17. Notwithstanding paragraphs 13 to 16, where the Flag CCP confirms that the ALC on board the vessel is functioning normally, but the Secretariat is not receiving the vessel's VMS position reports, the Secretariat shall immediately take steps to resolve any technical or other issue that is preventing it from receiving the VMS position reports. If the VMS position reports cannot be retrieved by the Secretariat after the issue has been resolved, the Flag CCP shall send these VMS position reports to the Secretariat via manual reporting and provide the Secretariat with any assistance as may be necessary.

Measures to prevent tampering with ALCs

18. Each CCP shall ensure that the ALCs fitted on board vessels flying their flag are tamper resistant, that is, are of a type of and configuration that prevent the input or output of false positions, and that they are not capable of being over-ridden, whether manually, electronically or otherwise, in accordance with the minimum standards for ALCs set out in Annex 1.

19. Each CCP shall prohibit vessels flying their flag to destroy, damage, switch off, render inoperative or otherwise interfere with the ALC.

20. In the event that a CCP or the Secretariat obtains information that indicates an ALC on board a fishing vessel operating in the Agreement Area does not meet the requirements of Annex 1 or there is evidence that the ALC has been tampered with, it shall immediately notify the Secretariat, and the fishing vessel's Flag CCP which shall:

    a) investigate the suspected breach of this measure as soon as possible; and

    b) depending on the outcome of the investigation, if necessary suspend the vessel from fishing until an ALC that meets the specifications outlined in Annex 1 is operational on board the vessel; and

    c) communicate actions taken to the Meeting of the Parties, including the outcome of the investigation within 30 days of its completion.

21. Nothing in this measure shall prevent a CCP from applying additional or more stringent measures to prevent tampering of ALCs on board vessels flying its flag.

Use and Release of VMS position reports

22. All requests for access to VMS position reports must be made to the Secretariat by a VMS Point of Contact by electronic means using the appropriate template[3] at least 5 working days in advance of the intended use, except for the purposes of paragraph 23 c), and in accordance with the procedures set out in paragraphs 24 to 29. The Secretariat shall only provide VMS data to a secure email address specified at the time of making a request for data.

23. Upon request of a CCP, the Secretariat shall only provide VMS position reports without the permission of the Flag CCP for the exclusive purposes of:

[3] The template shall be developed by the Secretariat and submitted to the Compliance Committee and the Meeting of the Parties for consideration.

a) planning for active surveillance operations and/or boarding and inspection at sea within 72 hours of the expected start of the operations in the Agreement Area;

b) active surveillance operations and/or boarding and inspection at sea in the Agreement Area;

c) supporting search and rescue activities undertaken by a competent Maritime Rescue Coordination Centre (MRCC) subject to the terms of an Arrangement between the Secretariat and the competent MRCC. Such Arrangement shall be reported to the Meeting of the Parties.

24. For the purpose of implementing paragraph 23 a) and b):

a) Boarding and inspection at sea shall be undertaken in accordance with CMM 14(2021) (High Seas Boarding and Inspection Procedures), including its paragraph 7;

b) each CCP shall only make available VMS position reports relevant to the planned or active surveillance operations and/or boarding and inspection at sea in the Agreement Area to the requesting CCP's inspectors and any other government officials for whom it is deemed necessary to access the reports;

c) CCPs shall ensure that such inspectors and government officials keep the VMS position reports confidential and only use the reports for the purposes described in paragraph 23 a) and b);

d) CCPs shall be allowed to retain VMS position reports provided by the Secretariat for the purposes described in paragraph 23 a) and b) until 72 hours after the time that the active operation has concluded. Except in the circumstances outlined in paragraph 24 e), CCPs shall submit a written confirmation to the Secretariat of the deletion of the VMS position reports immediately after the 72 hours' period;

e) CCPs' inspectors and government officials authorities shall be allowed to retain VMS position reports provided by the Secretariat for the purposes described in paragraph 23 a) and b) for longer than the periods specified in paragraph 24 d) only if it is part of an investigation, judicial or administrative proceeding of an alleged violation of the provisions of the Agreement, any CMMs or decisions adopted by the Meeting of the Parties. CCPs shall inform the Secretariat of the purposes and expected timing of the additional period of retention before the expiration of the initial period and the Secretariat shall promptly notify the concerned Flag CCP of the additional period. CCPs shall submit a written confirmation to the Secretariat of the deletion of the VMS position reports as soon as the purposes have been achieved or immediately after the additional period of retention has expired, whichever is earlier.

25. For the purpose of paragraph 23 a), CCPs requesting VMS position reports shall provide the Secretariat the geographic area of the planned surveillance and/or boarding and inspection activity. In this case, the Secretariat shall provide the most recent available VMS position reports for the notified geographic area at a specified point in time no more than 72 hours prior to the commencement of each surveillance and/or boarding and inspection activity. In the event that the planned surveillance and/or boarding and inspection activity does not proceed, the CCP shall notify the Secretariat, destroy the VMS position reports, and confirm their deletion to the Secretariat in writing, without delay. Regardless of whether the planned surveillance and/or boarding and inspection

activity were conducted or not, the Secretariat shall notify the Flag CCP that the VMS position reports were provided to the CCP no later than 7 days after the VMS position report provision, and, if applicable, that they have received confirmation that the reports have been deleted.

26. For the purpose of paragraph 23 b), the Secretariat shall provide VMS position reports from the previous 10 days, for vessels detected during the active surveillance and/or boarding and inspection activity by a CCP, and VMS position reports for all vessels within 300 n miles of the surveillance and/or boarding and inspection activity location. The Secretariat shall provide regular updates of VMS position reports to the CCP for the duration of the active surveillance and/or boarding and inspection activity. CCPs conducting the active surveillance and/or boarding and inspection activity shall provide the Secretariat and the VMS Point of Contact of the Flag CCP with a report including the name of the vessel or aircraft on active surveillance and/or boarding and inspection activity. This information shall be made available without undue delay after the surveillance and/or boarding and inspection activities are complete. The Secretariat shall notify the Flag CCP that the VMS position reports were provided to the CCP no later than 7 days after the active surveillance and/or boarding and inspection activity has ended, and, if applicable, that they have received confirmation that the reports have been deleted.

27. For the purpose of paragraph 23 c), upon the request of a CCP, the Secretariat shall provide VMS position reports without the permission of the Flag CCP for the purposes of supporting search and rescue activities undertaken by a competent MRCC subject to the arrangement between the Secretariat and the competent MRCC, including in relation to the provision of VMS position reports to the requesting CCP, and the protection and deletion of those reports.

28. Other than the purposes set out in paragraph 23, the Secretariat shall only provide VMS position reports to a requesting CCP or to the SIOFA Scientific Committee and its subsidiary bodies where the VMS position reports relates to vessels flagged to CCPs that have provided prior written consent through their VMS Point of Contact for the reports to be shared. CCPs shall destroy/delete requested VMS data, once the data has served its intended purpose, and confirm their deletion to the secretariat in writing, without delay.

29. CCPs may request VMS position reports for their own flagged vessels from the Secretariat.

Closed areas and interim protected areas

30. If VMS position reports received by the Secretariat indicates the presence of a fishing vessel in closed areas, or of a fishing vessel excluding those using line and trap methods in an interim protected area, as defined in paragraph 44 and Annex 3 of CMM 01(2023) (Interim Management of Bottom Fishing), the Secretariat shall notify the Flag CCP. The Flag CCP shall investigate the matter and provide an explanation within 5 working days to the Secretariat. The explanation shall be provided by the Secretariat to the Compliance Committee for consideration at its next annual meeting.

Data security and confidentiality

31. All CCPs, the Secretariat, the SIOFA Scientific Committee and its subsidiary bodies, and any SIOFA VMS provider shall ensure the secure and confidential treatment of VMS data, including ALC details in their respective electronic data processing facilities, in particular where the processing involves transmission over a network. CCPs and the Secretariat shall take appropriate measures to protect VMS data against accidental or unlawful destruction, loss alteration, unauthorized disclosure or access, and against all inappropriate form of processing.

32. The Meeting of the Parties shall adopt detailed data security and confidentiality provisions prior to the entry into operation of the SIOFA VMS and shall review the applicability and appropriateness of CMM 03(2016) (Data Confidentiality) to VMS position report security, confidentiality, management and use.

32 bis. CCPs and the Secretariat shall take necessary measures to comply with the agreed confidentiality and security provisions for the SIOFA VMS, [including applicable provisions under CMM 03.]

~~32.~~ 32 ter. The CCPs and the Secretariat shall only use VMS data for the purposes specified in this CMM.

Formatted: Indent: Left: 0.5", No bullets or

Entry into operation

33. The SIOFA VMS shall enter into operation at a date to be determined by the Meeting of the Parties.

34. Upon entry into operation of the SIOFA VMS, paragraphs 5 to 14 of CMM 10(2023) (Monitoring) shall be superseded and replaced by this CMM.

Review

35. Following the entry into operation of the SIOFA VMS, the Secretariat shall report annually to the Meeting of the Parties on the implementation of, and compliance with, this CMM, including measures taken to implement the confidentiality and Security requirements/measures/provisions.~~.~~

36. After two years of implementation, the Meeting of the Parties shall conduct a review of this CMM and consider improving it as appropriate.

Annex 1
Minimum standards for Automatic Location Communicators (ALCs) used in the SIOFA VMS

1. The Automatic Location Communicator (ALC) shall continuously, automatically and independently of any intervention by the fishing vessel, communicate VMS position reports referred to in paragraph 1(f) of this conservation measure.

2. The position reports referred to in paragraph 1(f) shall be obtained from a satellite-based positioning system.

3. ALCs fitted to fishing vessels must be capable of transmitting the position reports referred to in paragraph 1(f) recorded at least every fifteen minutes.

4. ALCs fitted to fishing vessels must be tamper-proof so as to preserve the security and integrity of the position reports referred to in paragraph 1(f).

5. Storage of information within the ALC must be safe, secure and integrated within a single unit under normal operating conditions.

6. It must not be reasonably possible for unauthorised persons to alter any of the VMS position reports stored in the ALC, including the frequency of position reporting to the FMC.

7. Any features built into the ALC or terminal software to assist with servicing shall not allow unauthorised access to any areas of the ALC that could potentially compromise the operation of the VMS.

8. ALCs shall be installed on fishing vessels in accordance with the manufacturer's specifications and applicable standards.

9. Under normal satellite navigation operating conditions, positions derived from the data forwarded must be accurate to within 100 metres (2 × Distance Root Mean Squared; 2DRMS) i.e., 99 per cent of the positions must be within this range.

10. The satellite navigation decoder and transmitter shall be fully integrated and housed in the same tamper-proof physical enclosure.

Formatted: Font: Not Bold

CMM 03(2016)[1]

Conservation and Management Measure for Data Confidentiality, Security measures, and Procedures for access and use of data (Data Confidentiality)

The Meeting of the Parties to the Southern Indian Ocean Fisheries Agreement;

RECOGNISING that Article 4(a) of the *Southern Indian Ocean Fisheries Agreement* (SIOFA or the Agreement) calls on the Contracting Parties, in giving effect to the duty to cooperate, to adopt measures on the basis of the best scientific evidence available to ensure the long-term conservation of fishery resources, taking into account the sustainable use of such resources and implementing an ecosystem approach to their management;

FURTHER RECOGNISING Article 11(3)(d) of the Agreement which provides that Contracting Parties shall collect and share in a timely manner, complete and accurate data concerning fishing activities by vessels flying its flag operating in the area, in particular on vessel position, retained catch, discarded catch and fishing effort, where appropriate maintaining confidentiality of data as it relates to the application of relevant national legislation; and

RECALLING Article 14 of the Agreement which calls on Contracting Parties to promote transparency in decision making processes and other activities carried out under the Agreement;

***ADOPTS* the following Conservation and Management Measure (CMM) in accordance with Article 6 of the Agreement:**

1. This CMM establishes the policy and procedures on confidentiality of data that will apply to data collected from Contracting Parties, cooperating non-Contracting Parties (CNCPs) and Participating Fishing Entities (PFEs) in accordance with the Agreement and relevant SIOFA CMMs.

1 bis. CCPs and the Secretariat shall take necessary measures to comply with these confidentiality and security measures.

Data Submitted to the Secretariat

2. The policy for releasing catch-and-effort, length-frequency, Vessel Monitoring System (VMS) Data, and observer data will be as follows:

Public domain data

a) The following data shall be considered to be "public domain data":

i) Data for vessels including current flag, name, registration number, international radio call sign, IHS-Fairplay (IMO) number, previous names, port of registry, previous flag, type of vessel, types of fishing methods, length, length type, gross tonnage (and/or gross registered tonnage), power of main engine(s), hold capacity, vessel authorisation start and end dates; and

[1] Obsolete references have been updated by 2023 technical edits.

Formatted: Font: Not Bold

ii) Observer data grouped by 5° longitude by 5° latitude, stratified by month and by flag State, provided that:

A. the catch of no individual vessel can be identified within a time/area stratum; and
B. the flag State that submitted the data provides its written authorisation that such data be considered to be "public domain data".

b) The following data shall be considered to be "public domain catch and effort data": Catch-and-effort and length-frequency data grouped by 5° longitude by 5° latitude by month stratified by fishing method associated with catch and flag State, provided that the catch of no individual vessel can be identified within a time/area stratum. In cases when an individual vessel can be identified, the data will be aggregated to preclude such identification, and will then be "public domain catch and effort data".

c) The Secretariat shall keep "public domain catch and effort data" confidential until the Meeting of the Parties has acted on the advice of the Scientific Committee in relation to a SIOFA Bottom Fishing Impact Assessment and SIOFA bottom fishing footprint as provided for under the Conservation and Management Measure for the Interim Management of Bottom Fishing in the SIOFA Agreement Area (CMM 01(2023)). This will not prevent observer data or finer scale catch and effort data being made available by the Secretariat to the Scientific Committee on a confidential basis where required.

d) The Secretariat shall compile and disseminate "public domain data", and "public domain catch and effort data" provided the conditions in paragraph 2(c) are satisfied, through appropriate mechanisms, including the SIOFA website, once developed.

Finer level stratification

e) Finer-scale data including catch and effort, length-frequency ~~and~~ observer data and VMS data will be made available to the Scientific Committee and any of its working groups, on a confidential basis, to undertake its work.

f) Catch and effort ~~and~~ length-frequency data, and VMS data grouped at a finer level of time-area stratification will only be released with written authorisation from the flag State that submitted the data. Except for VMS data, ~~E~~each such data release will also require the specific permission of the Secretariat.

g) Individuals requesting the data are required to provide a description of the research project, including the objectives, methodology and intentions for publication. Prior to publication, the manuscript should be cleared by the Secretariat. The data are released only for use in the specified research project and the data must be destroyed upon completion of the project. However, with written authorisation from the flag State that submitted the data, catch-and-effort and length-frequency data may be released for long-term usage for research purposes, and in such cases the data need not be destroyed.

h) The identity of individual vessels will be hidden in finer-level data unless the individual requesting this information can justify its necessity and the flag State that submitted the data provides its written authorisation.

i) Individuals requesting data shall provide a report of the results of the research project to the SIOFA Secretariat for subsequent forwarding to the sources of the data.

Formatted: Font: Not Bold

j) The Secretariat shall only provide confidential data to a secure email address specified at the time of making a request for data.

Procedures for the ~~safeguard~~safeguarding and securing of records

3. Procedures for safeguarding and securing records ~~and~~ , databases, and VMS Data will be as follows:

a) Access to logbook-level information ~~or~~ , detailed observer data or VMS data will be restricted to SIOFA staff members who require these records for their official duties. Each staff member having access to these records will be required to sign an attestation recognising the restrictions on the use and disclosure of the information.

b) Logbook and observer records will be kept locked, under the specific responsibility of the staff in charge of Data ~~Manager.~~ These sheets will only be released to authorised SIOFA staff members for the purpose of data input, editing or verification. Copies of these records will be authorised only for legitimate purposes and will be subjected to the same restrictions on access and storage as the originals.

c) Databases will be encrypted to preclude access by unauthorised persons. Full access to the database will be restricted to the staff in charge of Data ~~Manager~~ and to senior SIOFA staff members requiring access to these data for official purposes, under the authority of the SIOFA Executive Secretary. Staff entrusted with data input, editing and verification will be provided with access to those functions and data sets required for their work.

d) CCPs and the Secretariat shall take appropriate measures to protect all data against accidental or unlawful destruction, loss alteration, unauthorised disclosure or access, and against all inappropriate forms of processing.

3 bis. The following security measures shall be mandatory for the SIOFA VMS:

- System Access Control: the system has to withstand break-in attempts from unauthorised persons
- Authenticity and data access control: the system has to be able to limit access of unauthorised parties to only the data necessary for their task via a flexible user identification and password mechanism
- VMS data must be securely communicated: communication between CCPs, Service Provider, and the Secretariat shall use secure protocols in accordance with the VMS Specifications, Standards and Procedures (SSPs).
- Data Security: All VMS data received by the Secretariat shall be securely stored for a predetermined time, and shall not be tampered with
- Security Procedures: The Secretariat shall implement the Information System Security Policy to ensure proper access to the system (hardware and software), system administration and maintenance, backup and general usage of the system.

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

Formatted: Indent: Left: 0"

Data submitted to the Scientific Committee

4. Data submitted to the Scientific Committee and any of its working groups will be retained by the Secretariat or made available for other analyses only with the permission of the flag State that submitted the data.

Annex 3 – CMM 03 with Confidentiality and Security Measures

[5. The above rules of confidentiality will apply to all members of the Scientific Committee and any of its working groups.]

5 bis The Secretariat shall inform the MoP of measures taken to implement these confidentiality and security provisions.

Formatted: Font: Not Bold

Commented [JL1]: Propose deletion as para 1 bis implies same.