NPFC Data-Sharing and Data-Security Protocol for Vessel Monitoring System (VMS) Data

Definitions

1. For the purpose of this Protocol, unless specifically defined herein, words and terms have the same meaning as in the Convention on the Conservation and Management of High Seas Fisheries Resources in the North Pacific Ocean (Convention) and any conservation and management measures (CMMs) adopted by the North Pacific Fisheries Commission (Commission or NPFC), including in particular the CMM on the Vessel Monitoring System (VMS).

a) "Confidential" refers to non-public domain data and information held by Commission Members, the Secretariat, and by service providers contracted by the Commission, or contractors acting on their behalf, that is to be kept private, and shall not be accessed, released or disclosed unless such access, release or disclosure is for the purposes described in, and authorized by, this Protocol;

b) "Scientific purposes" may include estimating distribution of fishing effort for use in the Commission's research activities; planning for and implementing tagging programmes; modelling fishing effort for use in fisheries management activities, including management strategy evaluation (MSE); estimating abundance indices or undertaking stock assessments; validating logbook data; and, any other scientific purposes agreed to by the Commission.

Purpose

2. The purpose of this Protocol is to implement Article 16, paragraph 4 of the Convention, which states, "The Commission shall establish rules to ensure the security of, access to and dissemination of data, including data reported via real-time satellite position-fixing transmitters, while maintaining confidentiality where appropriate and taking due account of the domestic practices and domestic laws of members of the Commission."

Scope of Application

3. This Protocol applies to VMS data transmitted to, received by, stored, and, used by the Secretariat, the Commission and its Members, and authorized contractors, from authorized NPFC vessels in the Convention Area.

General Provisions

Accountability and Control System

4. All VMS data shall be considered confidential.

5. It is the responsibility of each Commission Member, and the Secretariat, to take all necessary measures to comply with this Protocol when transmitting and receiving VMS data.

6. Prior to accessing VMS data, authorized contractors shall be informed that VMS data is confidential and shall sign the Confidentiality Agreement (attached as Appendix 1) stipulating that they have been informed that the VMS data is confidential and that they have reviewed, are familiar with, and agree to the procedures to protect confidential VMS data set forth in the Confidentiality Agreement.

7. Where VMS data is transmitted by the Secretariat, with the approval of the Commission, to a party not already authorized to receive VMS data in accordance with this protocol, the Secretariat shall remain responsible for such data. The third party must receive written authorization from Secretariat to receive VMS data and shall be required to sign the Confidentiality Agreement (attached as Appendix 1). Breach of the Confidentiality Agreement constitutes breach of this Protocol, and will result in access to confidential VMS data being revoked, until corrective actions deemed appropriate by the Commission and the Secretariat have been taken. The third party will maintain the data provided to it in a manner no less stringent than the security standards established by the Commission.

8. The Executive Secretary will report to the Commission annually on the compliance with this Protocol, including any breach thereof.

Data Purposes

9. All VMS data collection, access, storage, use, and dissemination shall only be undertaken for the purposes of monitoring, control, and surveillance in the Convention Area, supporting search and rescue operations, and fulfilling the functions of the Commission, as established in Article 7(1) and (2) of the Convention, including scientific purposes as defined above, and subject to any additional relevant regulations, protocols, CMMs or policies approved by the Commission.

Safeguards

10. All authorized personnel having access to VMS data are prohibited from unauthorized use or disclosure of such data.

11. All VMS data shall be protected against loss or theft, as well as unauthorized access, dissemination, copying, use, or modification, by security safeguards, in accordance with the Data Retention and Security Section of this Protocol.

Data Access and Use

12. VMS data should only be accessed and/or used by authorized personnel in the Secretariat, authorized MCS entities and personnel, and authorized contractors, for the identified purposes in this Protocol or for other purposes identified by the Commission.

13. The Secretariat shall not make VMS data available to a Member where the Commission has established that the Member has not complied with this Protocol, or the CMM for VMS.

Use for Inspection Presence in Convention Area

14. For a Member who has an Inspection Presence in the Convention Area, VMS data shall be made available electronically in accordance with the following provisions:

a) Each Member shall identify a point of contact for VMS data;

b) Each Member who has an Inspection Presence in the Convention Area shall provide the Secretariat with the geographic area (in multiples of 10 degrees latitude and longitude with a north and south latitude boundary and an east and west longitude boundary) of the planned boarding and inspection MCS activities at least 72 hours in advance, when practicable;

c) Without prejudice and pursuant to CMM 2017-09, and following the notification process outlined above, the Secretariat shall make VMS data available electronically for the area defined in paragraph 14 b) as it is received, to each Member who has an Inspection Presence in the Convention Area. The provisions of this paragraph shall expire at the end of the next scheduled Commission meeting.

d) Each Member who has an Inspection Presence in the Convention Area shall only make VMS data available to authorities or inspectors, as defined in the CMM for High Seas Boarding and Inspection Procedures for the North Pacific Fisheries Commission (NPFC) responsible for fisheries monitoring, control, and surveillance activities in the Convention Area unless the data is being used in an investigation, or a judicial, or administrative proceeding, and subject to any relevant domestic laws and policies, and has requested VMS data in support of HSBI/MCS activities.

15. Where the fishing vessel to which the VMS data pertains has been involved in an alleged violation of a CMM, the Convention, or domestic laws or regulations, the VMS data pertaining to the alleged violation may be retained, and the Secretariat will be notified, by Members who have an inspection presence in the Convention Area until appropriate proceedings, including investigations, and judicial or administrative proceedings, have concluded.

16. Should no VMS data be retained pursuant to paragraph 15, each Member who has an Inspection Presence in the Convention Area shall delete all VMS data received from the Secretariat within seven days following the completion of monitoring, control, and surveillance activities in the Convention Area. The Member shall also submit a written confirmation to the Secretariat of the deletion of the VMS data within seven working days following the completion of monitoring, control, and surveillance activities.

Use for Search and Rescue Operations

17. For the purpose of supporting search and rescue operations by a Commission Member, the Secretariat shall make VMS data available upon request from a Member.

Data Retention and Security

Data Retention

18. All VMS data transmitted to the Secretariat in accordance with the Convention and CMMs shall be retained by the Secretariat.

19. Each Commission Member shall retain VMS data for fishing vessels flying its flag for at least one year.

Data Security

20. Each Commission Member and the Executive Secretary shall ensure the security of VMS data in their respective electronic data processing facilities, particularly where the use of VMS data involves transmission over a network.

21. Security measures must be appropriate to the level of risk posed by the transmission, processing, and storage of VMS data. At a minimum, the following security requirements must be implemented prior to transmitting or receiving VMS data:

a) The Executive Secretary shall ensure that regional system access to VMS data under its control is protected such that all data that enters the system is securely stored and will not be accessed by or tampered with from unauthorized individuals by implementing, at minimum, the following measures:

i. physical access to the computer system which transmits, uses, and stores VMS data is controlled;

ii. each user of the system is assigned a unique identification and associated password, and each time the user logs on to the system, he or she must provide the correct password;

iii. user access shall be audited annually for analysis and detection of security breaches; and

iv. each user shall be given access only to the data necessary for his or her task.

b) Data exchange protocols for electronic transmission of VMS data between Commission Members and the Secretariat shall be duly tested by the Secretariat and periodically reviewed by the Commission. Electronic transmission is subject to security procedures established in this Protocol.

c) Appropriate encryption protocols duly tested by the Secretariat and periodically reviewed by the Commission shall be applied by authorized contractors, including the use of cryptographic techniques to ensure confidentiality and authenticity.

d) Security procedures shall be designed by authorized contractors addressing access to the system hardware and software, system administration and maintenance, backup, and general usage of the system. Each Commission Member, and the Executive Secretary, shall ensure proper maintenance of system security and restrict access to the system accordingly. Each Commission Member shall liaise with the Secretariat in order to identify and resolve any security breaches or issues.