North Pacific Fisheries Commission

Original Version / COM07 March 2023

NPFC DATA SHARING AND DATA SECURITY PROTOCOL

Abstract:

This paper establishes a protocol for the access to, security and the dissemination of data held by the NPFC Secretariat. The protocol is guided by general principles that the Executive Secretary is responsible for management of data, that the data owners shall take responsibility for the identification of confidential data where it is necessary to do so and specifies a priority for the Commission to protect data and remind Members of their obligations to comply with the obligations outlined in the protocol. The protocol differentiates between public and non-public domain data and provides appendixes with examples to illustrate the types of data held by the secretariat. It provides rules for access to the different types of data, for data collection, storage, and dissemination. Further, a data request form/confidentiality agreement is annexed for the provision of access to confidential data.

2nd Floor Hakuyo Hall,
Tokyo University of Marine Science and Technology,
4-5-7 Konan, Minato-ku, Tokyo
108-8477, JAPAN

TEL +81-3-5479-8717
FAX +81-3-5479-8718
Email secretariat@npfc.int
Web www.npfc.int

NPFC DATA SHARING AND DATA SECURITY PROTOCOL

SECTION 1 – INTERPRETATION

1. This Protocol shall be interpreted, unless specifically defined herein, in accordance with the Convention and any Conservation and Management Measures (CMMs) adopted by the Commission.

2. The following definitions apply:

a) "data" includes both raw and processed information, including but not limited to electronic data files (regardless of their storage media and including hard copies, like discs or thumb drives, and data otherwise in transit), and information derived from processed data (regardless of the storage or presentation media). Data also includes technical reports, system documentation, user manuals, contracts, guidelines, and/or procedures;

b) "confidential data" refers to nonpublic domain data and information held by 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;

c) "public domain data" is data that is not confidential, including that which is already in the public domain through publication in electronic or print format. Public domain data excludes private information about individuals or information which can identify activities of any individuals, vessels, or companies.

d) "internal users" are defined as the Officers of the Commission, Commission committees and their subsidiary bodies, Members, Cooperating Non-Contracting Parties (CNCPs), the Secretariat, as well as authorized contractors, consultants, and/or service providers;

e) "external users" are defined as persons or organizations other than internal users, such as the public, non-governmental organizations (NGOs), academic and/or

research institutes, media, and other RFMOs with or without a Memorandum of Understanding (MOU) with the Commission; and

f) "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, estimating abundance indices or undertaking stock assessments, validating logbook data, and any other scientific purposes agreed to by the Commission.

SECTION 2 – PURPOSE

3. This Protocol, in accordance with Article 16 (4) of the Convention, establishes rules to ensure the security of, access to, and dissemination of data while maintaining confidentiality where appropriate and taking due account of the domestic law and practices of Members.

SECTION 3 – APPLICATION

4. This Protocol applies to all data collected by the Commission.

SECTION 4 – GENERAL PRINCIPLES

5. The Executive Secretary is responsible for the management of NPFC data received and held by the Secretariat in accordance with this Protocol.

6. The data owner, such as the Executive Secretary for the Secretariat, the Representative for the Member, or the author of a document not yet in the public domain, will be responsible for identifying confidential data along with any confidentiality requirements for their security, unless confidentiality is already made clear under this Protocol.

7. It is a priority of the Commission to protect Members' and the Commission's data, and to inform Members of their responsibility to protect, use, and disclose this data in an authorized manner.

8. The Commission will endeavor to make information relating to its Data Sharing and Data Security Protocols and procedures readily available to individuals, Members, CNCPs, or other parties.

SECTION 5 – DATA USE

Public Domain Data

9. There are no limitations on the use of public domain data. NPFC's public domain data may be accessed on its website and/or upon request.

10. Data released by the Secretariat to the public domain shall not reveal the individual activities of any vessel, company, or person, shall not disclose personal or business identities, and shall not contain confidential data, unless decided otherwise by the Commission. In this regard, catch and effort data in the public domain shall be made up of observations from a minimum of three vessels, unless the owner of the data decides otherwise.

11. Besides the data described in Paragraphs 8 and 9, examples of data listed in *Appendix 1* are considered to be public domain data.

12. The NPFC website should contain a statement describing the conditions associated with the viewing or downloading of public domain data (for example, that the source of the data must be acknowledged) and should require the person requesting the data to "accept" these conditions before viewing / downloading can begin.

13. The Secretariat is responsible for media releases in accordance with the decisions of the Commission.

Non-Public Domain Data

14. Subject to the decisions of the Commission, all types of data not described in Paragraph 10 shall be referred to as non-public domain data and considered to be confidential.

15. A list of examples of non-public domain data can be found in *Appendix 2*.

16. Access to and dissemination of non-public domain data shall be authorized in accordance with this Protocol.

17. The Secretariat shall log and report to the Commission all access by and dissemination to an external user of non-public domain data, including the name and affiliation of the person, the type of data accessed or disseminated, the purpose for which the data were requested, the date when the data were requested, the date when the data were released, and authorizations that may have been required.

18. The use of non-public data may occur under the following circumstances, unless otherwise specified in any CMMs and this Protocol.

a) Persons duly authorized by the Executive Secretary, including Secretariat staff, contractors, consultants, and service providers, shall have access to the data necessary to perform their NPFC duties. Officers of the Commission, Commission subcommittees, and their subsidiary bodies shall have access to the data necessary to perform their NPFC duties.

i. Secretariat staff, as part of their NPFC duties, are expected to keep non-public domain data confidential, are expected to be familiar with the procedures to protect confidential data, and are expected to understand that they will maintain the data security standards of the Commission. Such security responsibilities will be described to staff members when they start the position and are included in the terms and conditions of their employment.

ii. Any persons listed in (a), other than Secretariat staff, granted access to non-public domain data shall sign a Confidentiality Agreement (*Appendix 3*) with the Secretariat confirming that they have been informed that the data is confidential, that they have reviewed, and are familiar, with the procedures to protect confidential data, and that they will maintain the data security standards of the Commission in respect of data to which they have access. The Secretariat is to maintain a Register of all such persons (including the purpose for which they require access to the data) and make the Register available to Members upon written request.

b) Access to non-public domain data by Members and CNCPs

i. Members and CNCPs shall have access to non-public domain data to serve the purposes of the Convention, including data:
   - covering vessels flying their flag in the Convention Area
   - covering any vessels fishing in waters under their jurisdiction
   - covering vessels unloading in their ports or transshipping fisheries resources within waters under their jurisdiction

ii. Members and CNCPs shall notify the Secretariat of a small number of representatives (preferably limited to two) authorized to receive non-public domain data. Such notification will include name, affiliation, and contact information (e.g., telephone and email address). The Secretariat will maintain a list of such authorized representatives. Members and the Secretariat shall ensure the list of Members' representatives is kept up to date and made available.

iii. The authorized representative(s) of Members and CNCPs are responsible for ensuring the confidentiality and security of the non-public domain data in a manner consistent with security standards established by the Commission.

iv. The non-public domain data described in 18(b)(i). above will be made available by the Secretariat to authorized representatives of the Members and CNCPs upon request and, where appropriate, available to download by secure means from the Commission’s website.

v. Access to non-public domain data by Members and CNCPs shall be administered by the Executive Secretary on the basis of this protocol.

c) Exchange of data with other RFMO/As:

i. if the Commission enters into arrangements for the exchange of data with other RFMO/As, such arrangements may require the NPFC and the other RFMO/A to provide equivalent data on a reciprocal basis and maintain the

data provided in a manner consistent with the security standards established by the Commission; and

ii. at each annual meeting of the Commission, the Secretariat is to provide copies of data exchange arrangements that exist with other RFMO/As and a summary of the data exchanges that occurred during the previous twelve months under such arrangements.

d) Dissemination of non-public domain data in other circumstances

i. Non-public domain data will be made available by the Secretariat to any persons if the data owner authorizes the Commission to release them. In cases where a Member elects to provide an ongoing authorization for the release of such data, the Member may at any time cancel this authorization by notifying the Secretariat that it has revised its earlier decision. Unless otherwise requested by the provider of the data:

- Persons that request non-public domain data shall complete and sign the Data Request Form and sign the Confidentiality Agreement *(Appendix 3)* and provide them to the Commission in advance of obtaining access to said data.

- The completed and signed Data Request Form and Confidentiality Agreement shall then be forwarded to the Member that originally provided the requested data and the provider shall be requested to authorize the Commission to release the data. The Secretariat is to maintain a Register of all such persons (including the purpose for which they require access to the data) and make the Register available to Members upon written request.

- Such persons that request non-public domain data shall also agree to maintain the data requested in a manner consistent with the Section 7 on security standards, as established by the Commission.

ii. Members and CNCPs that have provided non-public domain data to the Commission shall notify the Secretariat of their representatives with the authority to authorize the release of non-public domain data by the Commission. Decisions whether to authorize the release of such data shall be made in a timely manner.

SECTION 6 – DATA COLLECTION AND MANAGEMENT FOR SPECIFIC PURPOSES

Scientific Data

19. Data collected or used for scientific purposes shall be collected, stored, accessed, used, and disseminated in accordance with the *Regulations for Management of Scientific Data and Information* developed by the Scientific Committee and approved by the Commission.

Monitoring, Control, Surveillance, and Enforcement Data

General Principles

20. Each Member's Representative, and the Executive Secretary, is responsible for the monitoring, control, surveillance, and enforcement data under its control. Member Representatives and/or the Executive Secretary may designate, in writing, others who are permitted to access this data and who would not otherwise be permitted to do so under this Protocol or the Convention through a Confidentiality Agreement, making such users accountable for compliance with this Protocol.

21. Where monitoring, control, surveillance, and enforcement data are provided to a third party, the individual providing the data shall remain responsible for such data. Monitoring, control, surveillance, and enforcement data shall only be provided to third parties with security safeguards equal to or greater than those enumerated in Section 7 of this Protocol.

22. Any monitoring, control, surveillance, and enforcement data received by the Commission from a third party, such as an RFMO, shall be considered Commission data or information, and therefore be protected in a manner consistent with this Protocol.

23. All monitoring, control, surveillance, and enforcement data shall be considered confidential data and shall be protected in a manner appropriate to their sensitivity. In establishing appropriate safeguards, attention should be given to ensuring reasonable availability and utility of monitoring, control, surveillance, and enforcement data in order to fulfill the functions of the Commission, while more sensitive information should be safeguarded by a higher level of protection.

24. All monitoring, control, surveillance, and enforcement data collected and managed by the Commission, including the Secretariat, under any CMM will be protected and accessed in accordance with the principles in this protocol, unless otherwise stated in a specific CMM. Further considerations for specific data types are outlined below.

Vessel Monitoring System

25. Vessel monitoring system data shall be collected, stored, accessed, used, and disseminated in accordance with the NPFC Data-Sharing and Data-Security Protocols for Vessel Monitoring System (VMS) Data.

High Seas Boarding and Inspection Reports and Violation Case Package

26. Boarding reports and violation information shall be treated as confidential data, subject to any domestic legal disclosure requirements, and shared in accordance with the HSBI CMM as established by the Commission.

27. Data related to boarding and inspection operations, including potential violations, may be disseminated, in accordance with this protocol, to other authorized inspection vessels and inspectors as necessary for carrying out monitoring, control, surveillance, and enforcement responsibilities in the Convention Area, unless such data is being used in an investigation, judicial, or administrative proceeding, and subject to consent by the inspecting Member and any relevant domestic laws and policies.

28. Members may request data covered in this Protocol for fishing vessels under the Member's jurisdiction, as well as vessels applying to conduct fishing activities in the Member's national waters, unload in the Member's ports, or transship within waters under the Member's jurisdiction, for the purposes of monitoring, control, surveillance and enforcement.

29. Boarding and inspection reports and violation case data must be collected, stored, and reported in a standardized format. They must comply with the time requirements specified by the Commission, as well with as the HSBI CMM content requirements.

30. Security safeguards established by the authorized inspector and authorized inspection vessel for boarding and inspection reports and violation case data must include measures to ensure the integrity and authenticity of such data, and particularly during transmission of the boarding and inspection reports and violation case data between authorized inspectors and other authorized recipients.

Vessel License and Registration

31. All vessel register data, including those pertaining to fishing vessels authorized for fishing activities in the Convention Area, and authorized inspection vessels and authorities or inspectors, will be securely maintained, and made available in accordance with relevant CMMs as established by the Commission.

32. Under the CMM on Vessel Registration, Members and CNCPs shall ensure they have maintained the NPFC Vessel Registry and shall make the record publicly available as appropriate and subject to any legal confidentiality regulations of the individual Member and CNCP. The Commission shall provide to any Member or CNCPs, upon request, information about any vessel entered on the Commission record that is not otherwise publicly available, per *Appendix 2*.

33. All additions, modifications, or removal of data or information from vessel registers must be logged.

Illegal, Unreported, and Unregulated Fishing Vessel Data and Information

34. Illegal, unreported, and unregulated vessel and fishing data will be made available for external users only in accordance with the CMM To Establish a List of Vessels Presumed to Have Carried Out IUU Activities in the Convention Area.

SECTION 7 – DATA SECURITY

Confidential Data Transmission

35. Confidential data must be transmitted using secure transmission methods.

36. Each Member, CNCP and the Executive Secretary shall ensure the security of data in their respective electronic data processing facilities, particularly where the use of data involves transmission over a network. Security measures must be appropriate to the level of sensitivity posed by the transmission, processing, and storage of the confidential data.

Data Access and Storage

37. The Executive Secretary shall implement, at a minimum, the following measures to ensure that access to data under the control of the Secretariat 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::

a. physical access to the computer system which transmits, uses, and stores data is controlled;
b. 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;
c. user access shall be audited annually for analysis and detection of security breaches; and
d. each user shall be given access only to the data necessary for his or her task.

38. Hard copies of data will be stored in a secure area within the offices of the Secretariat and will physically be protected from unauthorized access, damage, and/or interference.

Data Warehousing and Lifecycle

39. Data collected by or transmitted to the Secretariat under the Convention or CMM requirements (i.e. data in annual reports, VMS) will be held in perpetuity.

40. Data maintained by the Secretariat will be annually backed-up to a secure server and all back-up copies of data will be tracked.

Asset Management

41. The Executive Secretary, for the Secretariat, is the primary owner of Commission data, unless otherwise specified. As the owner of Commission data, the Executive Secretary remains responsible for the protection of data, to periodically review the maintenance of the data, and to ensure that it is being kept in accordance with this protocol.

Reporting of Security Incidents

42. All users of NPFC data are required to report any information on security breaches, possible breaches, weaknesses, or other issues as quickly as possible to the Secretariat.

Appendix 1

Examples of Public Domain Data

a) The data described in Article 16(2) of the Convention;

b) annual catch estimates stratified by gear, flag, and species, and number of fishing days;

c) catch and effort data aggregated by gear type, flag, year/month, and 5° latitude and 5° longitude, where applicable – and made up of observations from a minimum of three vessels;

d) biological data (if adequate time has passed to allow the scientists that organised for the collection of such data to publish a paper analysing it);

e) the NPFC Vessel Registry;

f) information on vessel and gear attributes compiled from other sources;

g) oceanographic and meteorological data;

h) Section 1 of the Annual Report to the Commission by Members.

i) IUU vessel list;

j) for purposes of HSBI transparency, name of inspection vessel, and flag state of vessel boarded in accordance with HSBI CMM procedures;

k) final Compliance Report and Executive Summary; and

l) any other types of data that the Commission decides to make publicly available.

Appendix 2

Examples of Non-Public Domain Data

a) operational level catch and effort data;

b) operational level landing data;

c) operational level transshipment data;

d) data describing (at a fine resolution) the movement of vessels, including near real time vessel position, direction and speed (this includes Commission VMS data);

e) boarding and inspection reports;

f) observer reports;

g) certified inspection personnel;

h) port state inspection reports;

i) violations and infringements, detailed;

j) Section 2 and 3 of the Annual Report to the Commission by Members;

k) data that reveals the individual activities of any vessel, company, or person;

l) draft and provisional compliance reports and all associated documentation;

m) any other data classified as non-public domain data in accordance with the domestic requirements of Members; and

n) any other types of data that the Commission decides not to make publicly available.

Appendix 3

Data Request Form and Confidentiality Agreement:
for individuals seeking access to non-public data held by the Secretariat

Please include the name(s), contact information, and signature(s) of the authorized representative(s) (attaching an additional sheet if necessary) for whom access to the data is being requested; the use of the non-public domain data shall be authorised only for the person(s) listed below]

Full Name	**Agency/Organization,** **Address, Email, & Phone**	**Signature and Date**

In return for the NPFC Secretariat granting me access to non-public NPFC data, I hereby make the following declarations and promises:

1. I am requesting access to NPFC data:

    a. for the following purposes (provide a detailed explanation, attaching an additional sheet if necessary):

2. I have read, understood, and will abide by the NPFC Data Sharing and Data Security Protocol ("Protocol"). I understand that the data I am requesting are confidential, as defined in the Protocol. I agree to abide by the provisions of the Protocol that address protecting and safeguarding this data.

3. I agree to abide by any additional written conditions regarding the use of this data that the Secretariat attaches to this Confidentiality Agreement.

4. I agree that this data shall be used only for the purposes for which I have requested, accessed only by me and other individuals who have signed a Confidentiality Agreement, and will be destroyed within seven days upon completion of the usage for which the data are being requested. I further agree to report the destruction of data to the Secretariat.
5. I agree to make no unauthorized copies of this data. If a copy of all, or part, of the data is made by me, all copies, and/or parts thereof, will be registered with the Secretariat and will be destroyed within seven days upon completion of the purpose for which I requested the data
6. Prior to the publication of any report in which I intend to use requested this data, I agree to provide the report to the Secretariat for clearance to ensure that no data will be published.
7. I agree to provide a copy of any published reports referenced in paragraph 6 to the Secretariat.
8. I agree not to disclose, divulge, or transfer, either directly or indirectly, the requested data to any third party without the prior written consent of the Secretariat.
9. I agree to promptly notify the Secretariat, in writing, of any unauthorized or inadvertent disclosure of this data.
10. I assume all liability, if any, with respect to my breach of this Confidentiality Agreement after I receive the requested data.
11. In the event of my breach of this Confidentiality Agreement, I understand that the Secretariat will not grant me access to data until corrective actions deemed appropriate by

the Secretariat have been taken by me, my employer, or by the Member under whose supervision I work.

This Agreement is effective on the date indicated below upon signature of an authorized representative of the Secretariat.

_____ _____

Authorized NPFC Secretariat Representative Date