NPFC-2020-SC05-WP06

**Draft - NPFC Data Sharing and Data Security Protocols**

TCC Small Working Group on Planning and Development

(as of 29 October 2020)

*Abstract:* TCC Small Working Group on Planning and Development (TWG PD) drafted a general NPFC data management and use protocol. While it is still under development by the TWG OP, the SC is invited to review the draft protocol and provide recommendations to the TCC and the Commission. It is proposed that data collected or used for scientific purposes shall be collected, stored, accessed, used, and disseminated in accordance with the existing *Interim Regulations for Management of Scientific Data and Information* (paragraph 11).

**Draft - NPFC Data Sharing and Data Security Protocols**

**Definitions**

1. For the purposes of interpreting these measures and procedures, the following definitions apply:
2. “Confidential” means data that are kept private and cannot be accessed or disclosed without authority.
3. “Commission” refers to the North Pacific Fisheries Commission, established under Article 5(1) of the Convention;
4. “Convention” refers to the *Convention on the Conservation and Management of High Seas Fisheries Resources in the North Pacific Ocean*;
5. “Convention Area” refers to the area of application of the Convention, established under Article 4(1) of the Convention;
6. “Data” means raw and processed data, electronic data files (regardless of their storage media and including hard copies 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. Data types are outlined in Section 5 of this policy.
   1. “Internal” users are defined as Commission Committees and their subsidiary bodies, Members, Secretariat, and authorized contractors/consultants/service providers.
   2. “Internal use” of data is the use of data by internal users for conducting Commission business under the Convention.
   3. “External” data users are defined as the public, ENGOs, non-Members, media, and other RFMOs with or without MOUs with the Commission.
   4. “External data use” is the use of data by external data users.
7. “Inspection Presence in the Convention Area” means the Member is authorized by the High Seas Boarding Inspection Procedure to conduct inspections and is planning for or actively engaged in surveillance in the Convention Area;

**Purpose**

1. This policy is intended to implement Article 16, paragraph 1 of the Convention, which provides that the Commission “shall, taking full account of Annex I of the 1995 Agreement as well as relevant provisions of Articles 10 and 11, develop standards, rules, and procedures for, *inter alia”*:
2. the collection, verification and timely reporting to the Commission of all relevant data by members of the Commission;
3. the compilation and management by the Commission of accurate and complete data to facilitate effective stock assessment for ensuring that the provision of the best scientific advice is enabled;
4. the exchange of data among members of the Commission, and with other regional fisheries management organizations and arrangements, and other relevant organizations including data concerning vessels engaged in IUU fishing and, as appropriate, concerning the beneficial ownership of those vessels, with a view to consolidating that information into a centralized format for dissemination as appropriate;
5. the facilitation of coordinated documentation and data-sharing between regional fisheries management organizations and arrangements, including procedures to exchange data on vessel registers, and market-related measures where applicable; and,
6. regular audits of Commission member compliance with data collection and exchange
7. It is a priority of the Commission to protect Member and organizational information, and to inform Members of their responsibility to protect, use, and disclose information in an authorized manner.
8. This policy establishes rules to ensure the privacy of confidential data and prohibits access to and dissemination of confidential data except in accordance with this policy, while taking due account of the domestic laws applicable to members of the Commission.

**Scope**

1. This policy applies to all users of NPFC Secretariat data.
2. This policy applies to data collected under the NPFC Convention and information derived from such data.

**General Principles**

1. The Secretariat is responsible for the management of NPFC data, information, and documents in accordance with this policy.
2. The information owner, such as the Member, will be responsible for identifying confidential data, information, or documents, along with any confidentiality requirements for their data, information, or documents.

**Data Types and Uses**

1. Non-Public Domain Data
2. The Secretariat is to have access to the data necessary to perform relevant duties on behalf of the Commission.
3. Authorized users of public domain data may cite or use Commission-related data when working on matters under consideration by the Commission or its subsidiary bodies.
4. Public Domain Data
5. External data use by other RFMOs may occur under either of the following circumstances:
6. If the Commission enters into arrangements for the exchange of data with other RFMOs, such arrangements may require that the partnering RFMO provide equivalent data on a reciprocal basis and maintain the data provided to them in a manner consistent with the security standards established by the Commission.
7. At each annual meeting of the Commission, the Secretariat is to provide copies of data exchange arrangements that exist with other RFMOs and a summary of the data exchanges that occurred during the previous 12 months under such arrangements.

**Data Collection and Management**

1. Data collected or used for scientific purposes shall be collected, stored, accessed, used, and disseminated in accordance with the Commission’s *Interim Regulations for Management of Scientific Data and Information*.

**Monitoring, Compliance, and Enforcement Data**

**General Principles for Monitoring, Compliance and Enforcement Data**

*Accountability*

1. Each Commission Member, and the Secretariat, is responsible for the monitoring, control, surveillance and enforcement data under its control, and shall designate an individual or individuals who are accountable for its compliance with this Protocol.
2. Where monitoring, control, surveillance and enforcement data are provided to a third party by a Commission Member or the Secretariat, the Commission Member or Secretariat shall remain responsible for such data. Monitoring, compliance, and enforcement data should only be provided to third parties with security safeguards equal to or greater than those enumerated in this Policy.
3. Any monitoring, control, surveillance and enforcement data and information 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 Policy.

*Security Safeguards*

1. All monitoring, compliance, and enforcement data and information shall be protected in a manner appropriate to its sensitivity. More sensitive information should be safeguarded by a higher level of protection.

*Utility*

1. In establishing appropriate safeguards, attention should be given to ensuring reasonable availability and utility of monitoring, compliance, and enforcement data and information in order to fulfill the functions of the Commission.

*Transparency*

1. The Commission will endeavor to make information relating to its data and information policies and procedures readily available to individuals, Commission Members, or other parties in a manner that is generally understandable.

**Vessel Monitoring System**

1. Vessel monitoring system data shall be collected, stored, accessed, used, and disseminated in accordance with the Commission’s *Vessel Monitoring System Data and Information Security Protocol*.

**High Seas Boarding and Inspection Reports and Violation Case Package**

1. Boarding reports and violation case information shall be treated as confidential information, subject to any domestic legal disclosure requirements, and shared in accordance with conservation and management measures (CMMs) as established by the Commission.
2. Data or information related to boarding and inspection operations, including potential violations, may be disseminated to other authorized vessels and inspectors as necessary for carrying out monitoring, compliance, and enforcement responsibilities in the Convention Area, unless such data or information is being used in an investigation, judicial, or administrative proceeding, and subject to any relevant domestic laws and policies.
3. Authorized inspection vessels and authorized inspectors may request data or information covered in this Policy for fishing vessels under the Member’s jurisdiction and 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.
4. Boarding and inspection reports and violation case information must be collected, stored, and reported in a standardized format and by time requirements as specified by the Commission.
5. Security safeguards for boarding and inspection reports and violation case information must include measures to ensure the integrity and authenticity of such data and information, and particularly during transmission of the boarding and inspection reports and violation case between authorized inspectors and other authorized recipients.

**Observer Data and Information**

1. [Reserved]

**Vessel License and Registration**

1. 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.
2. All additions, modifications, or removal of data or information from vessel registers must be logged and reported.

**Illegal, Unreported, and Unregulated Fishing Vessel Data and Information**

1. Illegal, unreported, and unregulated vessel and fishing data will be securely maintained in a manner consistent with its sensitivity.
2. Illegal, unreported, and unregulated vessel and fishing data will be externally published only in accordance with the CMM for listing of illegal, unreported, and unregulated vessels.

**Externally Available Data**

1. Data in the public domain released by the Commission shall not reveal the individual activities of any vessel, company or person and shall not contain confidential information.
2. Pursuant to Article 16, section 2 of the Convention, the following data are to be made publicly available:
3. the number of fishing vessels operating in the Convention Area
4. the status of fisheries resources managed under the Convention
5. fisheries resources assessments
6. research programs in the Convention Area
7. cooperative initiatives with regional and global organizations.
8. Annual Reports
9. Annual Reports submitted in accordance with article 16(3) of the Convention are to be available to external users through the NPFC website.
10. Media Releases
11. The Secretariat is responsible for media releases.

**Data Security**

1. Data Transmission  
   1. Data must be transmitted using secure transmission methods.
2. Data Warehousing & Lifecycle  
   1. Data collected by or transmitted to the Secretariat under Convention or CMM requirements (i.e. data in annual reports, VMS) will be held in perpetuity.
3. Confidentiality
   1. Data identified as confidential by members are to remain confidential, unless authorized for dissemination in accordance with this policy.
   2. Authorized contractors with access to data shall be informed of its confidentiality and shall sign the Confidentiality Agreement (to be attached as Appendix 1 when developed), confirming that they have been informed that the data is confidential and that they have reviewed, and are familiar, with the procedures to protect confidential data.
   3. Any persons, contractors, or officers granted access to confidential data shall sign a Confidentiality Agreement with the Secretariat and 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.
4. Access to and Dissemination of Data
5. Data may be disseminated if the CMM requiring the data collection authorizes its release, or in accordance with this policy.
6. Data ordinarily kept confidential may be released if the Member providing the data expressly authorizes the release.
7. If a Member or cooperating non-Member wishes to cite and/or use Commission-related data for work that is intended to be conducted or shared outside of the NPFC, such Member or non-Member should consult with the data provider(s) through the Secretariat, stating 1) the data subject to the request, and 2) the purpose for which the data are intended to be used. The Secretariat should immediately notify the data provider(s) of the request. The data provider(s) should inform the Secretariat within 30 calendar days whether to accept or reject the request. If the data provider(s) reject the request, the data provider(s) should state the reason(s) for the rejection. If the data provider(s) accept the request, the data provider(s) may request an agreed-upon credit line in any subsequently-created product. Those who cited/used data should not distribute the data further nor use it for the purpose not declared.