DATA CONFIDENTIALITY POLICY AND PROCEDURES

SUBMITTED BY: UK(OT) AND CO-SPONSORED BY MALDIVES, MOZAMBIQUE, SEYCHELLES, 1 MAY 2014

Explanatory Memorandum

To address the data confidentiality and security requirements associated with a companion proposal submitted by the UK(OT) and co-sponsored by the Maldives, Mozambique and the Seychelles (IOTC–2014–S18–PropI) we also propose to update Resolution 12/02 *Data confidentiality policy and procedures* to include VMS data, as follows.

RESOLUTION 14/XX ~~12/02~~
DATA CONFIDENTIALITY POLICY AND PROCEDURES

The Indian Ocean Tuna Commission (IOTC),

RECOGNISING the need for confidentiality at the commercial and organisational levels for data submitted to the IOTC;

CONSIDERING the provisions set forth in Resolution 10/02 *mandatory statistical requirements for IOTC Members and Cooperating Non-Contracting Parties (CPCs)*;

CONSIDERING the provisions set forth in Resolution 11/04 *on a regional observer scheme*;

CONSIDERING the provisions set forth in Resolution 14/XX *on the vessel monitoring system (VMS) programme*;

ADOPTS in accordance with paragraph 1 of Article IX of the IOTC Agreement, that:

1. The following policy and procedures on confidentiality of data will apply:

DATA SUBMITTED TO THE IOTC SECRETARIAT

2. The policy for releasing catch-and-effort, length-frequency and observer data will be as follows:

Standard stratification

a) Catch-and-effort and length-frequency data grouped by 5° longitude by 5° latitude by month for longline and 1° longitude by 1° latitude by month for surface fisheries stratified by fishing nation are considered to be in the public domain, 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 by time, area or flag to preclude such identification, and will then be in the public domain.

Finer level stratification

b) Catch-and-effort and length-frequency data grouped at a finer level of time-area stratification will only be released with written authorisation from the sources of the data. Each data release will require the specific permission of the IOTC Executive Secretary;

c) Observer data grouped by 1° longitude by 1° latitude for surface fisheries and by 5° longitude by 5° latitude for longline, stratified by month and by fishing nation are considered to be in the public domain, provided that the activities /catch of no individual vessel can be identified within a time/area stratum;

d) A Working Party will specify the reasons for which the data are required;

e) 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 IOTC Executive Secretary. 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 authorisation from the sources of 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;

f) The identity of individual vessels will be hidden in fine-level data unless the individual requesting this information can justify its necessity;

g) Both IOTC Working Parties and individuals requesting data shall provide a report of the results of the research project to the IOTC for subsequent forwarding to the sources of the data.

3. The policy for releasing tagging data will be as follows:

   a) Detailed tagging and recovery data are considered to be in the public domain, with the exception of any vessel names or identifiers and detailed information about the person who recovered the tag (name and address), however, requests for tagging data should be made to the IOTC Executive Secretary through the application form provided at **Annex I**.

PROCEDURES FOR THE SAFEGUARD OF RECORDS

4. Procedures for safeguarding records and databases will be as follows:

   a) Access to logbook-level information or detailed observer data will be restricted to IOTC staff requiring 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 Data Manager. These sheets will only be released to authorised IOTC personnel 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 Data Manager and to senior IOTC staff requiring access to these data for official purposes, under the authority of the IOTC 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.

DATA SUBMITTED TO IOTC WORKING PARTIES AND THE IOTC SCIENTIFIC COMMITTEE

5. Data submitted to IOTC Working Parties and the IOTC Scientific Committee will be retained by the IOTC Secretariat or made available for other analyses only with the permission of the source.

6. The above rules of confidentiality will apply to all members of IOTC Working Parties and the IOTC Scientific Committee.

VESSEL MONITORING SYSTEM (VMS) DATA SUBMITTED TO A CENTRALISED VESSEL MONITORING SYSTEM

7. VMS data submitted to the Commission by flag States will be stored at the Commission with the utmost security as described in para 4.

8. VMS data will be considered as highly confidential.

9. VMS data will only be forwarded from the Commission to a CPC coastal State when the State can show it has met the necessary security criteria outlined in paragraph 11 to ensure the confidentiality of flag State VMS data.

10. Data will be forwarded to coastal States only when a vessel is present inside a coastal State's waters.

11. VMS data shall be considered to be confidential and Contracting Parties (Members) of the Commission which receive VMS data from flag States shall adopt secure information technology procedures and systems to ensure that the confidentiality of VMS data is maintained. This shall include as a minimum standard the following:

Physical Security

   a) The coastal State Fisheries Monitoring Centre (FMC) shall be housed in a physically secure location that ensures that only certain personnel can access the VMS data provided;

b) VMS servers shall also be housed in a physically secure location if remote from the FMC;

Personnel

c) A register of personnel permitted access to the VMS and the levels of access granted shall be maintained by the coastal State FMC;

d) These personnel shall have appropriate training relating to the use of the VMS and data security issues of the data provided;

e) Other agencies or personnel to whom data access will be granted shall be highlighted e.g. restricted access to VMS data may be granted to other governmental organisations for actions such as search and rescue operations in addition to law enforcement duties;

f) In the event an outside technician is required, the technician shall be supervised and observed at all times by a member of the coastal State FMC staff;

Electronic Security

g) A system of network and database security including individual user passwords shall be employed to ensure only registered personnel can access the local areas networks, physical hardware and software through which the VMS data provided;

h) Only system administrators shall have full access to the system;

i) Other users' access privileges shall be limited to only those necessary to fulfil their job requirements;

j) Where possible, systems should log access and maintain transaction logging on all changeable data;

Data Confidentiality

k) Operational policies shall be developed to ensure that the data are protected from damage or disclosure;

l) This policy shall outline all measures which the coastal State has implemented.

12. This Resolution supersedes Resolution 12/02 *Data Confidentiality Policy and Procedures*.

~~7. This Resolution supersedes Resolution 98/02 *Data Confidentiality Policy and Procedures*.~~

ANNEX I
TAGGING DATA USERS APPLICATION FORM

To the Executive Secretary of the Indian Ocean Tuna Commission

I wish to submit the following request to receive and analyse data from the Indian Ocean Tuna Tagging Programme. I have read the above Data Users Policy, noting in particular, the matters relating to data confidentiality and providing an appropriate acknowledgement in the case of any publications arising from the use of these data, and agree to all the conditions listed.

Name of the institution/s requesting the data and contact details for the head researcher
Project outline
Specifications of the data required
Names and positions of the staff accessing the data (*Note, the IOTC Secretariat expects to be informed of any changes to the data users list*)
Intentions with respect to publication of the results of the proposed work

Signature and date:

Name:

Position:

Organisation:

Approved / Not Approved

Signature and date:

IOTC Executive Secretary: