

RESOLUTION 98/02

DATA CONFIDENTIALITY POLICY AND PROCEDURES

Recognizing the need for confidentiality at the commercial and organisational levels for data submitted to IOTC, the following policy and procedures on confidentiality of data will apply:

DATA SUBMITTED TO THE SECRETARIAT

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

- 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.
- 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 Secretary.
 - a) A Working Party will specify the reasons for which the data are required.
 - b) 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 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.
 - c) The identity of individual vessels will be hidden in fine-level data unless the individual requesting this information can justify its necessity.
 - d) Both Working Parties and individuals requesting data shall provide a report of the results of the research project to IOTC for subsequent forwarding to the sources of the data.

PROCEDURES FOR THE SAFEGUARD OF RECORDS

Procedures for safeguarding records and databases will be as follows:

- Access to logbook-level information 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.
- Logbook 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.
- 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 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 WORKING PARTIES

- Data submitted to Working Parties will be retained by the Secretariat or made available for other analyses only with the permission of the source.
- The above rules of confidentiality will apply to all members of Working Parties.