**RES-GFCM/35/2011/1**

# on data confidentiality policy and procedures, amending Resolution GFCM/30/2006/1

The General Fisheries Commission for the Mediterranean (GFCM),

*RECOGNISING* the need for confidentiality at the commercial and organizational levels for data, reports and messages submitted to GFCM;

***ADOPTS***, in accordance with paragraph 1 (h) of Article III and with Article V of the GFCM Agreement, the following policy and procedures on confidentiality of data:

## 1. Field of application

The provisions set out below shall apply to all data, reports and messages (electronic and of other nature) transmitted and received pursuant to GFCM recommendations.

## 2. General provisions

a) The Executive Secretary and the appropriate authorities of the Contracting Parties and Cooperating non-Contracting Parties (CPCs) , transmitting and receiving data, reports and messages shall take all necessary measures to comply with the security and confidentiality provisions set out under paragraphs 3 and 4 of the present Resolution;

b) The Executive Secretary shall inform all CPCs of the measures taken by the Secretariat to comply with these security and confidentiality provisions;

c) The Executive Secretary shall take all the necessary steps to ensure that the requirements pertaining to the deletion of data, reports and messages handled by the Secretariat are complied with;

d) Each CPC shall guarantee the Executive Secretary the right to obtain as appropriate, the rectification of data, reports and messages the processing of which does not comply with the provisions of the GFCM Agreement;

e) The Commission may instruct the Executive Secretary not to make available the data, reports and messages submitted to the GFCM by a CPC, where it is established that the CPCs in question has not complied with these security and confidentiality provisions.

## 3. Provisions on data confidentiality

a) Data, reports and messages shall be used only for purposes stipulated in GFCM Recommendations.

b) (i) With respect to data provided under Recommendation GFCM/33/2009/3, the Secretariat shall develop web-based data access and reporting facilities which should be available, in accordance with the provisions of paragraph 4 (b), only to:

- Registered users nominated by the Contracting Party, without any time restrictions unless specified. This nomination could be revoked at any time by the Contracting Party,

- Registered participants of GFCM meetings with access limited to the period of the respective meetings.

(ii) General statistical reports and publications shall be made available to the general public without any restriction, in accordance with the guidance of the Commission and the security provisions of paragraph 4.

## 4. Provisions on data security

a) CPCs and the Executive Secretary shall ensure the secure treatments of data, reports and messages, in particular where the processing involves transmission over an electronic network. CPCs and the Executive Secretary must implement appropriate technical and organisational measures to protect data, reports and messages against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all inappropriate forms of processing.

The following security issues must be addressed from the outset:

- System access control: the system has to withstand a break-in attempt from unauthorised persons;
- Authenticity and data access control: the system has to be able to limit the access of authorised parties to a predefined set of data only;
- Communication security: it shall be guaranteed that data, reports and messages that enter the system are securely communicated;
- Data security: it shall be guaranteed that data, reports and messages that enter the system are securely stored for the required time and that they will not be tampered with;
- Security procedures: security procedures shall be designed addressing access to the system, system administration and maintenance, backup and general use of the system.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing of the data, reports and messages.

b) Data security

Access limitation to the data shall be secured via a flexible user identification and password mechanism. Each user shall be given access only to the data necessary for his task.

c) Security procedures

Each CPC and the Executive Secretary shall nominate a security system administrator. The security system administrator shall review the log files generated by the software, properly maintain the system security, restrict access to the system as deemed needed and act as a liaison with the Executive Secretary in order to solve security matters.