The Southern Indian Ocean Fisheries Agreement (SIOFA) 6th Meeting of the Parties
01-05 July 2019

Pearle Beach Resort & Spa conference centre, Flic en Flac, Mauritius

MoP6-Doc09

Protocols for the secure transfer of confidential data

Relates to agenda item: 13.5

Proposal □ Working Document □ Information Paper □ Other Document ☒

SIOFA Secretariat

Abstract

At SC3, SIOFA Database Manager was requested to investigate and implement protocols for the secure transfer of confidential data. Depending on the files size to be transferred and users' preferences, two procedures are proposed.

The 'Secretariat Policy for Ensuring Data Confidentiality' produced and circulated earlier in 2019 is provided at Annex I.

MoP is invited to consider these protocols and make any suggestions for improvements

Introduction

CMM 2016/03 provide information on the status of data (confidential vs public domain). The confidentiality and the security of data must be maintained during the whole process of the data (production, storage, exchange, storage). This document focuses on the exchange steps.

The Data Manager recommends that the exchange of confidential data is done during physical meeting. One person giving directly the data to another using a physical drive.

It not always possible nor relevant to have such arrangements to exchange data. Thus 2 options are proposed below to ensure a better security during data exchanges.

A. Email and phone

1. The sender need to encrypt the file; an easy way is to make a password protected archive file (using one of the many archive software providers such as *7z*).

2. The file can be sent by email if of reasonable size.
Note: Sometime email security policies will not allow email that contains encrypted attachments to be received. In such case, the email procedure cannot be used.

3. The recipient detach the file to a local computer drive and delete the message.

4. The sender provide the password to the recipient by a different way (not by email) like a phone call.

5. The recipient can then decrypt and use the file provided.

B. FTP Server

1. The Sender upload the file to a private FTP server folder (the sender can also encrypt the file for additional security).

3. The Sender provide the FTP link of the file to the recipient. The link can be provided by email.

4. The Sender provide the FTP credentials (username, password) to the recipient using a different way than the one used to give the FTP link. He can also provide the decryption password if required at that time.

5. The recipient download the file from the FTP server (using the credential provided).

6. The recipient can then use the file (after having decrypted if it was initially encrypted).

7. When the file has been downloaded, the recipient notify the sender, who can the file from the server and eventually cancel/shutdown the FTP service.

Conclusions and recommendations

Adopting these procedures will make the transfer of files more cumbersome, but it should prevent exposing confidential data during the transfer period. These methods do not involve too complex technologies. The FTP method is the best to deal with big files but need some knowledge on how to setup and manage FTP servers.

The use of online sharing services is not recommended as nobody can be sure the providing companies do not use the data sent into their servers. In a way the file encryption would guarantee a certain security, but an encrypted file would be more attractive to hackers than a plain file.

Any user must also be aware of his responsibility in regards of data confidentiality. The computer or any device where such data are stored must be safe and -if possible- not connected to any networks.

ANNEX 1

Secretariat Policy for Ensuring Data Confidentiality

SIOFA CMM 2016/03 Data Confidentiality establishes the policy and procedures on confidentiality of data that will apply to data collected from Contracting Parties, cooperating non-Contracting Parties (CNCPs) and Participating Fishing Entities (PFEs) in accordance with the Agreement and relevant SIOFA CMMs and held by the SIOFA Secretariat.

To provide further insurance that data confidentiality will be maintained the following measures will be taken within the SIOFA Secretariat:

If there is a requirement to communicate any fisheries data outside the Secretariat, the Secretariat shall follow this procedure:

1. The data manager (DM) prepares the dataset and assesses whether it constitutes non-public domain data or non-public domain catch or effort data.

2. If the assessment by the DM detects confidentiality issues the dataset will not be communicated and the person who requested the data will be informed.

3. If the assessment by the DM did not detect confidentiality issues, the data manager will inform the Executive Secretary (ES) and provide him/her with the dataset.

4. The ES will also check the dataset for any confidentiality issues.

5. If the ES has doubt about the confidentiality, he/she shall inform the DM.

6. If the ES agrees the data has no confidentiality issue, he/she can authorize the DM to transmit the dataset to the requesting person.

7. If the ES and DM find that the data requested may be non-public domain data or non-public domain catch or effort data, the ES should contact the primary data custodian to discuss possible options for the release of the data for specific purposes following the steps provided below). This may include aggregating data such that confidentiality is not breached.

If confidential dataset still needs to be provided to achieve SIOFA activities and objectives, then these steps shall be followed:

1. The relevant flag state/s will be informed of the work to be undertaken and asked if they agree to release data for the only purpose of this work.

2. If the flag state disagrees, the dataset will not be transmitted, and the requesting person informed by the DM.

3. If the flag state agrees, the DM will encrypt the dataset.

4. The DM will send the encrypted file/s to the requesting person along with a copy of CMM 2016-03, a statement advising that in accordance with CMM 2016/03 para 2g the data must not be released and destroyed upon completion of the project. The requesting person will be required to acknowledge and confirm acceptance of these conditions and confirm when the data has been destroyed.

5. Following receiving acceptance of conditions provided in paragraph 3 above, the DM shall communicate to the requesting person the key to decrypt the file by another means than that used to send the file (e.g. phone call).