SC-04-26

4th Meeting of the Southern Indian Ocean Fisheries Agreement (SIOFA) Scientific Committee

25-29 March 2019, Yokohama, Japan

Protocols for the secure transfer of confidential data

Please note that National Reports and SC Working Group reports shall be classified as working papers

Relates to agenda item: 5.3 Working paper ☒ Info paper □

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.

Recommendations

SC to consider the two procedures presented and provide any comments/addition. SC to determine if there are any objections implementing the procedures.

Introduction

It is recommended that the exchange of confidential digital data is managed during physical meeting. One person giving directly the data to another using a physical drive.

It not always easy nor relevant to have such arrangement to exchange data. Thus 2 options are proposed below to achieve this.

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 attachment 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 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 Sender copy the file to a private FTP account with a specific username and password on a server.

3. The Sender provide the link to the recipient to the FTP account. The link can be provided by email if the file is encrypted.

4. The Sender provide the password to the recipient using a different way than the one used to give the FTP credentials.

5. The recipient download the file from the FTP server.

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

7. When the file has been downloaded, the sender removes the file from the server and eventually cancel the FTP account and 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 to their systems. 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 where such data are stored must be safe and -if possible- not connected to any networks.