



CCSBT-EC/1110/17

CONFIDENTIALITY OF DATA AND DOCUMENTS

Purpose

To consider pending issues on the CCSBT confidentiality rules and to determine whether the reports of meetings and any documents produced for meetings related to CCSBT18 should be restricted from public release.

(1) Pending issues on CCSBT Confidentiality Arrangements

CCSBT 17 agreed to the “Rules and Procedures for the Protection, Access to, and Dissemination of Data Compiled by the CCSBT” for immediate application. These rules are provided at Attachment A. However, three paragraphs of the rules (5c, 21 and 22) were not implemented at CCSBT 17 and it was decided that these three paragraphs would be discussed before CCSBT 18. These three paragraphs are square bracketed and shaded in Attachment A.

The first two of these paragraphs (5c and 21) relate to compliance purposes and the issue with these paragraphs is the use of the words “high seas”, in that some Members feel this is appropriate while others believe that all waters should be included, not just high seas.

The third paragraph (22) relates to making VMS data available for scientific purposes and at least one Member does not have the flexibility to provide VMS data for scientific purposes.

These paragraphs were discussed at the Special Meeting. A proposal was made that these paragraphs be deleted from the rules¹ and that the words “under these rules” be appended to the title of Section 1 of the rules. It was agreed that CCSBT 18 would review the inclusion of these paragraphs.

(2) Confidentiality of reports and documents from 2011

Rule 10 of the Rules of Procedure provides that the reports prepared of Extended Commission meetings will be made available for public release unless a Member makes a request to restrict its release. Such a request must be made before adoption of the report of the Extended Commission. Restrictions on release of a report require a decision from the Extended Commission.

Documents submitted to Extended Commission meetings are also to be made available for public release unless the document contains previously restricted information, or unless the author of the document or the Member (if the author is a representative of a Member) makes a request to restrict its release. Such a request must be made before adoption of the report of the Extended Commission.

¹ Because these paragraphs all require separate rules to be developed and agreed, so they currently serve no purpose.

The 2006 Farm and Market review reports have been classified as confidential and consequently other documents that include estimates of unreported catches derived from these documents must also be kept confidential, including:

- A catch table incorporating this information that was prepared by the Secretariat and included in the material considered at the 2011 meeting of the Extended Scientific Committee. The Secretariat requests that Attachment A of this paper (CCSBT-ESC/1107/04) be treated as confidential.

At the time of writing this document, no other documents have been nominated to the Secretariat as having a confidential status.

**RULES AND PROCEDURES FOR THE PROTECTION, ACCESS TO,
AND DISSEMINATION OF DATA COMPILED BY THE CCSBT**

1. Basic principles relating to the dissemination of data by the CCSBT

1. Data and information specified in Table 1 and held by the CCSBT or its Secretariat, and by service providers or contractors acting on their behalf, shall only be released in accordance with these Rules and Procedures.
2. Notwithstanding paragraph 1, data may be released if the Member (or Cooperating Non-Member) of the Extended Commission providing the data to the CCSBT authorises its release.
3. Persons duly authorised by the Executive Secretary within the CCSBT Secretariat¹ and service providers, who have read and signed the Commission's confidentiality protocol, shall have access to the data necessary to perform their CCSBT duties.
4. Officers of the Commission² and its subsidiary bodies, who have read and signed the Commission's confidentiality protocol, shall have access to the data necessary to perform their CCSBT duties.
5. Members and Cooperating Non-Members (CNM) of the Extended Commission shall have access to data to serve the purposes of the Convention, including data:
 - (a) covering vessels flying their flag that were authorised or engaged in fishing for, retaining on board, transhipping or landing southern bluefin tuna.
 - (b) covering any vessels fishing in waters under their jurisdiction for the time period during which such fishing occurred.
 - (c) [subject to paragraph 21, for the purpose of compliance activities on the high seas that are consistent with the Convention and Conservation and Management Measures and other relevant decisions adopted by the Commission]
 - (d) for the purpose of scientific and other research, if the Member or CNM of the Extended Commission that originally provided that data authorises the Extended Commission to release them or if the data have a "No risk" or "Low" confidentiality risk classification according to Table 1³. In cases where a Member or CNM of the Extended Commission elects to provide an ongoing authorisation for the release of such data, the Member or CNM may at any time cancel this authorisation by notifying the Secretariat that it has revised its earlier decision.
6. To the greatest extent practical, the CCSBT, its Secretariat and their service providers or contractors acting on their behalf, should release data in a timely manner.

¹ Persons duly authorised by the Executive Secretary within the CCSBT Secretariat are Secretariat staff and contractors that are appointed by the Executive Secretary that are responsible to the Executive Secretary.

² Officers of the Commission are people appointed by the Commission (e.g. Independent Chairs, Scientific Advisory Panel) to perform a specific function for the Commission and are responsible to the Commission for this function.

³ These data are typically made available to Members through the private area of the CCSBT web site or the CCSBT Data CD.

2. Risk classification and definition of confidentiality

7. Data covered by these Rules and Procedures will be classified in accordance with the risk classification methodology included in **Table 1**, which reflects *inter alia* the damage that would be done to the operations or credibility of the Extended Commission as a consequence of the unauthorised disclosure of such information.
8. Data covered by these Rules and Procedures are determined to be either public domain or non-public domain data in accordance with the confidentiality risk classification established in **Table 1**.

3. Dissemination of Public Domain Data

9. Except for data as described in Paragraph 10, the types of data listed in Table 1 with a “No risk” classification have been designated to be Public Domain data.
10. Data in the public domain shall not reveal the individual activities or identity of any vessel, entity or person. Catch and Effort data in the public domain shall be aggregated by flag, gear, year, month and 1°x1° grid (for surface fisheries) or 5°x5° grid (for longline fisheries) and, provided that the data contains information on the number of vessels in a strata, shall be made up of observations from a minimum of three vessels.
11. Public Domain data shall be available to any persons for (a) downloading from the Commission’s website and/or (b) release by the Commission on request.
12. The Commission’s website should contain a statement describing the conditions associated with the viewing or downloading of Public Domain data (for example, that the source of the data must be acknowledged), and should require the person requesting the data to “Accept” these conditions before viewing or downloading can begin.

4. Dissemination of Non-Public Domain Data

4.1 Definition of Non-Public Domain Data

13. Subject to the decisions of the Extended Commission, all types of data not described in paragraph 9 shall be referred to as Non-Public Domain data.

4.2 General rules for dissemination of, and access to, Non-Public Domain data

14. All access to and dissemination of Non-Public Domain data shall only be authorised in accordance with these Rules and Procedures and shall be protected in accordance with the CCSBT Data Security Standards specified in **Attachment 1**.
15. The CCSBT Secretariat shall log and report to the Extended Commission all access and release of Non-Public Domain data with a “Medium” or High” risk classification including where applicable, the name and affiliation of the person, the type of data

accessed or released, the purpose for which the data were requested, the date when the data were requested, the date when the data were released and authorisations that were provided.

4.3 Access to Non-Public Domain data by the Staff of the Secretariat, the CCSBT Service Providers, and Officers of the Commission and its Subsidiary Bodies

16. Pursuant to paragraphs 3 and 4, persons duly authorised by the Executive Secretary, within the CCSBT Secretariat and service providers, including the scientific advisory panel, shall have access to the data necessary to perform their CCSBT duties. Officers of the Commission and its subsidiary bodies shall have access to the data necessary to perform their CCSBT duties. All such persons shall sign a Confidentiality Agreement with the Executive Secretary and maintain the CCSBT Data Security Standards in respect of data to which they have access. The Executive Secretary shall maintain a Register of all such persons (including the purpose for which they require access to the data) and make the Register available to a Member or CNM of the Extended Commission on written request.

4.4 Access to Non-Public Domain data by Members and CNMs of the Extended Commission

17. Members and CNMs of the Extended Commission shall have access to Non-Public Domain data to serve the purposes of the Convention, including data:

- (a) Covering vessels flying their flag that were authorised or engaged in fishing for, retaining on board, transshipping or landing southern bluefin tuna.
- (b) Covering any vessels fishing in waters under their jurisdiction for the time period during which such fishing occurred.
- (c) For the purpose of scientific and other research, if the Member or CNM of the Extended Commission that originally provided that data authorises the Extended Commission to release them or if the data have a “Low” confidentiality risk classification according to Table 1³. In cases where a Member or CNM of the Extended Commission elects to provide an ongoing authorisation for the release of such data, the Member or CNM may at any time cancel this authorisation by notifying the Secretariat that it has revised its earlier decision.

18. Members and CNMs of the Extended Commission shall notify the Secretariat of a small number of representatives (preferably only 2) authorised to submit requests⁴ for access to Non-Public Domain data. Such notification will include name, affiliation, and contact information (e.g. telephone, facsimile, email address). The CCSBT Secretariat will maintain a list of such authorised representatives. Members and CNMs of the Extended Commission and the Secretariat shall ensure the list of Member and CNM representatives is kept up to date and made available.

19. The authorised representative(s) of the Members and CNMs of the Extended Commission are responsible for ensuring the confidentiality and security of the Non-Public Domain

⁴ The requests by the authorised representatives would usually be to grant access to data for other people (e.g. scientists), not for themselves. For data classified with a “low risk”, the only requests that need to be made are requests for access to relevant parts of the private area of the CCSBT web site. These requests can be handled by simple e-mail correspondence directly with the Secretariat. For data with a “medium” or “high” risk, the procedures in Attachment 2 must be followed.

data according to its risk classification and in a manner consistent with the CCSBT Data Security Standards.

21. [For the purpose of compliance activities on the high seas, the Extended Commission will adopt separate rules and procedures for the access and dissemination of Non-Public Domain data.]
22. [VMS data will be made available for scientific purposes, subject to the separate rules and procedures referred to in paragraph 21 above.]
23. Access to Non-Public Domain data by Members and CNMs of the Extended Commission shall be administered and authorised by the Executive Secretary on the basis of these Rules and Procedures in conjunction with the Procedures for Requesting the Release of Non-Public Domain data at **Attachment 2**.
25. A Member or CNM that has not fulfilled its obligations to provide data to the Extended Commission for two consecutive years shall not be granted access to Non-Public Domain data until all such obligations are met. A Member or CNM whose representative, authorised in accordance with paragraphs 18 and 19 above, failed to observe the rules stipulated in these Rules and Procedures shall not be granted access to Non-Public Domain data until appropriate actions have been taken.

4.5 Exchange of data with other regional fisheries management organisations

27. If the Commission enters into agreements for the exchange of data with other regional fisheries management organisations (RFMOs) or other organisations, such agreements must include requirements that the other RFMO provides equivalent data on a reciprocal basis and maintains the data provided to them in a manner consistent with the CCSBT Data Security Standards. The data that may be exchanged are data with a risk classification of “no risk” or “low risk”. Data with higher risk classifications may only be considered for sharing after specific approval from the Extended Commission. At each annual session the Executive Secretary will provide copies of data exchange agreements that exist with other RFMOs and a summary of the data exchanges that occurred during the previous 12 months under such agreements.

4.5 Disseminations of Non-Public Domain data in other circumstances

26. Non-Public Domain data will be made available by the Secretariat to any persons⁵ if the Member or CNM of the Extended Commission that originally provided that data authorises the Extended Commission to release them. In cases where a Member or CNM of the Extended Commission elects to provide an ongoing authorisation for the release of such data, the Member or CNM may at any time cancel this authorisation by notifying the Secretariat that it has revised its earlier decision.
27. Conditions for access to Non-Public Domain data by each non-Member shall be determined on a case by case basis by the Member or CNM of the Extended Commission that originally provided the data. At the discretion of that Member or CNM, these conditions may or may not involve procedures similar to those specified at **Attachment 2**.

⁵ Including universities, researchers, NGOs, media, consultants, industry, federations, etc.

4.6 Force majeure

28. The Executive Secretary may authorise the release of Non-Public Domain data to rescue agencies in cases of *force majeure* in which the safety of life at sea is at risk.

5. Periodic Review

29. The Extended Commission or its subsidiary bodies will periodically review these Rules and Procedures, and subsidiary documents, and the rules and procedures referred to in paragraphs 21 and 22 above, and amend these if necessary.

30. When considering the provision of data not specified in Table 1, the Extended Commission or its subsidiary bodies should consider an appropriate risk classification for that data for inclusion in Table 1.

6. Final Clause

31. These Rules and Procedures do not prevent a Member or CNM from authorising the release of any data it has provided to the CCSBT.

Table 1: Types of information and confidentiality risk classification.

Information types that have not received a risk classification within this table will not be managed within these confidentiality rules. However, this table may be updated by the Extended Commission from time to time, including through intercessional agreement between Members of the Extended Commission, as required.

With the exception of approved summaries of certain information types below, the following broad dissemination principles apply to the four confidentiality risk classifications⁶:

- “No risk”: Publicly available and may be placed on the public area of the CCSBT web site.
- “Low Risk”: Not publicly available. However, it is available to all Members and CNMs without specific approval and may be placed on the private area of the CCSBT web site and on the CCSBT Data CD.
- “Medium Risk”: Not publicly available. Requires specific authorisation to be released. May not be placed on the CCSBT Data CD or on the private area of the CCSBT web site (unless in a special part of the private area that is further restricted to specifically authorised people).
- “High Risk”: Not publicly available. Requires specific authorisation to be released. May not be placed on the CCSBT Data CD or on the private area of the CCSBT web site.

Information Type	Risk Classification
Annual catch estimates and number of vessels stratified by gear and flag	No risk
Annual number of active SBT vessels, by gear type and flag ⁷	No risk
Aggregated catch and effort data stratified by gear/year/month, 5x5 (LL) or 1x1 (surface), and flag – and made up of observations from a minimum of three vessels in those cases where the data contains information on the number of vessels in a strata.	No risk
CCSBT Records of Authorised Fishing Vessels, Carrier Vessels & Farms	No risk
Aerial survey, SAPUE and troll indices	No risk
Biological data (catch at size and age data)	No risk ⁸ - Low
Biological data (gender, direct aging, otoliths, stomach contents, maturity, genetic data, isotopic N15/C14 collected by samples)	Low
Conventional Tagging data	No risk ⁹ - Low
Aggregated SBT catch and effort data stratified by gear/year/month, 5x5 (LL) or 1x1 (surface), and flag, with no minimum number of vessels	Low
Aggregated catch and effort data of other species stratified by gear/year/month, 5x5 (LL) or 1x1 (surface), and flag, with no minimum number of vessels	Medium
Other data and information specified by the Extended Scientific Committee (and subsequently approved by the Extended Commission) for the routine Scientific Data Exchange that have not been explicitly identified elsewhere in this table	Low
Monthly catch reporting by flag	Low
Authorised CDS Validators	Low ¹⁰
Initial quota allocations and final catch by vessel/company	Medium

⁶ The four risk classifications are also differentiated by the required level of security that applies to each classification as specified in the CCSBT Data Confidentiality Security Policy.

⁷ This information does not currently exist, but will become available once the CDS has been in operation for 12 months.

⁸ Catch at size and age data are considered to public after the annual Commission meeting each year. Other biological data are only considered public if adequate time has passed to allow the scientists that organised the collection of such data to publish a paper analysing it.

⁹ Only data from the CCSBT operated tagging program are considered to be “No risk”.

¹⁰ Also available to non-Members that are cooperating with the CCSBT CDS.

Information Type	Risk Classification
Aggregated catch and effort data for longline at a 1x1 resolution, with no minimum number of vessels ¹¹	Medium
Transshipment consignments	Medium
Certified transshipment observer personnel	Medium
Catch Documentation Scheme and Trade Information Scheme	Medium
Farming growth rates and tag seeding data	High
Individual SBT length data from stereo video observation of farm transfers	High
Operational level catch and/or effort data ¹²	High
Aggregated Scientific observer data other than biological data specified above, including for seabirds, turtles and marine mammals	Medium
Operational level Scientific observer data other than biological data specified above	High

¹¹ As part of the annual data exchange, the Secretariat provides aggregated catch effort data at this resolution for New Zealand from the operational level data New Zealand provides.

¹² Including target and/or non-target catch, this information is currently only provided by New Zealand.

Table 2: Annotations on information types mentioned in Table 1.

Information Type	Annotations
CCSBT Records of Vessels & Farms	Covers vessels & farms authorised to farm, fish and carry SBT.
Vessel and gear attributes from other open sources	Includes data collected by observers and port inspectors. Covers all vessels (i.e. includes vessels restricted to national jurisdiction–domestic fleets). Includes electronic equipment.
Oceanographic and meteorological data	“Oceanographic and meteorological data” in this context does not include information identifying the fishing vessel that collected the information, for example, which would otherwise alter its security classification.
Aerial survey, SAPUE and troll indices	Recruitment indices derived from aerial surveys (both scientific and commercial spotting – SAPUE stands for Surface Abundance Per Unit Effort) and scientific troll surveys.
Biological data	Biological data include catch at size and age data, data on gender and maturity, genetic data, direct aging and data on hard parts such as otoliths, stomach contents, and isotopic N15/C14 data collected by observers, port samplers and other sources. “Biological data” in this context does not include information identifying the fishing vessel, for example, which would otherwise alter its security classification.
Conventional Tagging data	Conventional Tagging data include release and recapture positions, lengths and dates. “No risk” Tagging data does not include information identifying the fishing vessel, company or individual that recaptured the tagged tuna (not even coded identifiers), for example, which would otherwise alter its security classification.
Other data and information specified by the Extended Scientific Committee (and subsequently approved by the Extended Commission) for the routine Scientific Data Exchange that have not been explicitly identified elsewhere in this table	Each year the Extended Scientific Committee (ESC) reviews the scientific Data Exchange Requirements for the following year and produces a table defining the types of data that are to be exchanged. The present information type relates to all information in that table produced by the ESC that are not explicitly classified elsewhere in Table 1 of these rules ¹³ . Any restrictions on the use of data specified in the Data Exchange requirements are to be observed in addition to following the procedures required for this data’s classification within Table 1 of these rules.
Monthly catch reporting by flag	CCSBT reporting system where monthly catches shall be reported by Members and CNMs one month after the month fishing.
Initial quota allocations and final catch by vessel/company	CCSBT reporting system where Members and CNMs report the quota initially allocated to each vessel/company and the final catch for the season of each vessel/company.
Catch Documentation Scheme and Trade Information Scheme	Data collected through the CCSBT Catch Documentation and Trade Information Schemes
Operational level Catch Effort data	Non-aggregated, set by set data collected on fishing vessel logbooks and by observers.
Electronic tagging data	Detailed electronic tagging data include detailed records from pop-up or archival tags such as date, time, depth, temperature, light intensity, etc.
Certified inspection personnel	If identified by individual then Risk Classification would be assigned to HIGH.
Violations and infringements, detailed	May cover Individual Violations and infringements pending investigation and/or prosecution. Includes compliance information collected by observers.
Economic & Social data	Insufficient information currently available to determine Risk Classification.

¹³ For example, the following items usually appear in the scientific Data Exchange requirements but are not specifically listed within these rules: recreational catch estimates, SBT import statistics, mortality allowance usage, non-retained catches, CPUE indexes etc.

CCSBT Data Confidentiality Security Policy (DCSP)

The purpose of this policy is to help ensure that non-public data (within this attachment only, non-public data is referred to as “Data”) is provided to and managed by Data receivers in a manner that maintains confidentiality. This policy is not intended to cover aspects of data security that are not related to protection of confidentiality, such as loss or damage to data (e.g. through fire, flood, accident, systems malfunction etc.).

Data receivers (including the CCSBT Secretariat) are required to manage the security of Data to at least the standards specified below. The standards below are intentionally brief in order to provide a clear overview of the scope of the requirements. Further information can be obtained on most items from ISO/IEC 27002:2005(e)¹⁴.

The Executive Secretary may impose additional security requirements before releasing specific Data. The receiver of the Data will be required to observe any such additional security requirements. The Executive Secretary may also waive specific security requirements if requested to do so by the provider of the Data.

1) Human Resources Security

- For data with a risk classification of “medium” or “high”, only people approved by the Executive Secretary (herein referred to as “Approved People”) shall be allowed access to the Data by the receiving organisation (herein referred to as “The Organisation”). For data with a “low” risk classification, people approved by the receiving Member or CNM shall be allowed to access the data (also referred to herein as “Approved People”).;
- The Organisation shall have appropriate terms and conditions in its contract/arrangement with Approved People to state their responsibilities for information security and to enable disciplinary action for Approved People who commit a security breach.
- Approved People shall be provided, as appropriate, with information security awareness education and training by The Organisation.
- The Organisation shall have termination procedures in place for maintaining confidentiality from Approved People whose role or employment changes. This will include as a minimum, the return or secure disposal¹⁵ of the Data, cancellation of access to the Data by such approved people, and for Approved People with approval for access to “medium” and High” risk data, notification to the Executive Secretary of the person’s changed status together with the action taken.

¹⁴ International Standard on “Information technology – Security techniques – Code of practise for information security management”.

¹⁵ For data with a “medium” or “high” risk classification, “Secure Disposal” means that media containing the data should be disposed of through incineration or shredding of paper records and by physically destroying electronic media or deleting the information by overwriting the Data using techniques that make the original information non-retrievable rather than using standard delete or format functions. Secure Disposal of “medium” and “high” risk data requires all copies of the Data, including any backups, to be destroyed. For Data with a “low” risk classification, the disposal procedures required for higher risk Data can be adjusted to a more practical process providing that such processes maintain confidentiality. For example, instead of destroying backups containing low risk Data, it would be sufficient to keep those backups in a secure environment with procedures in place that prevented unauthorised access to the Data on those backups.

2) Physical and Environmental Security

- Any unencrypted Data and products of that Data shall be stored in a physically secure area which will at minimum consist of:
 - a robust security perimeter¹⁶ and properly functioning entry controls (such as automatic locks with card controlled entry or manned reception desk) that prevent entry of unaccompanied non-approved people into the secure area; and
 - A properly functioning and monitored electronic intruder detection system that will detect an intrusion into the secure area.
- Data with a low to medium confidentiality classification and products of that Data that are encrypted as described in paragraph “5”, may be used in a non-public area outside the secure area described above. When not in use, the media containing these encrypted Data shall be carried in person, or stored in a locked private facility and secured or hidden out of sight.
- Equipment used for displaying the Data (such as monitors and printers) shall be located and positioned in such a manner as to prevent unauthorised viewing, recording or copying of the displayed information. Printouts of the Data or products of the Data shall be removed from printers immediately.
- The Data shall be Securely Disposed¹⁵ of:
 - for “medium” and “high” risk data, when the purpose for which the data were requested has been completed;
 - for all data, when the data are no longer required by the Organisation to serve the purposes of the Convention;
 - from any media that are scheduled for maintenance by non-Approved People and from any media prior to its disposal.

3) Communication and Operations Management

- Precautions shall be in place to detect and prevent the introduction of malicious code (such as computer viruses, Trojan horses and logic bombs) and unauthorised mobile code. These precautions will at least include:
 - Installation and regular (daily or less) update of malicious code detection and repair software to scan computers, media and e-mails for malicious code; and
 - The Organisation shall conduct education awareness campaigns, as appropriate, on the dangers of malicious code and how to reduce the risk of infection by malicious code.
- Appropriate network controls shall be implemented to maintain security for any Data that is accessible through the network.
- Cabling carrying the Data shall be protected from interception.
- The Data shall not be transmitted on public networks (such as the internet) unless the Data has been appropriately encrypted.
- Unencrypted Data shall not be transmitted on wireless networks unless the network is a private encrypted network and the Data has a low confidentiality classification. A computer that is connected to a wireless network may not contain Data with a medium or high confidentiality classification unless the Data are encrypted and the encrypted volume is not mounted (not active) while the computer is connected to the wireless network.
- Any actual or suspected security incidents shall be investigated and reported to the Executive Secretary.

¹⁶ A ground floor office with windows would require additional protection for the windows, or physically secure internal enclosures for the security perimeter to be acceptable.

4) Access Control

- Access to the Data shall require successful logon by an Approved Person, involving a User ID and Password¹⁷.
- The User ID shall be unique to the specific Approved Person.
- The Password must be kept confidential to the Approved Person only and should be subject to a suitable password management policy, including:
 - Provision of any temporary passwords in a secure manner and forcing passwords to be changed on first log on;
 - Forcing use of minimal length and complexity of passwords;
 - Prevent re-use of passwords;
 - Advising users to use quality passwords (easy to remember without writing down, not based on information that is easy to guess, not vulnerable to dictionary attacks, free of consecutive identical or sequential characters, contain both letters and numbers and have an acceptable minimum length) and changing passwords whenever there is an indication of possible password or system compromise, and at regular intervals;
 - Storing, transmitting and displaying passwords in protected (e.g. encrypted) form; and
 - Limiting the number of unsuccessful log-on attempts to only 3 and rejecting further attempts without specific authorisation.
- Accounts of Approved People shall be protected when unattended by use of a password protected screen saver¹⁸ that activates after less than 10 minutes of inactivity.

5) Cryptographic Control

- The Data shall be encrypted using robust encryption techniques whenever it is not in a physically secure area as described in paragraph “2” above.
- Provision or transmission of Data by the Secretariat to data receivers or to the private area of the CCSBT web site¹⁹ shall use encryption techniques (encrypted files or encrypted transmission protocols).
- Encryption may use either secret key techniques or public key techniques where each user has a public and a private key. For both types of techniques, a wide variety of suitable file encryption software is available for purchase (such as PGP) or for free (such as TrueCrypt).
- Encrypted volumes shall be automatically dismounted when there has been no activity (reading/writing to the encrypted volume) for 60 minutes, after entering a power saving mode, and when the user logs off.
- Secret and private keys shall be protected from unauthorised disclosure and shall be distributed to intended users in a secure manner.

¹⁷ Other technologies for identification and authentication such as biometrics (e.g. finger-print verification) may be used.

¹⁸ Or equivalent measure.

¹⁹ Unless otherwise agreed by the provider of the Data, only Data with a medium confidentiality classification or less may be placed on the private area of the CCSBT web site. However, Data with a medium confidentiality classification must be placed in a further restricted part of the private area that can only be accessed by people specifically authorised to access that Data.

Procedures for Requesting the Release of Non-Public Domain Data

1. Member's and CNM's of the Extended Commission that have provided Non-Public Domain data to the CCSBT shall notify the Secretariat regarding their representatives with the authority to authorise the release of Non-Public Domain data by the CCSBT. Decisions whether to authorise the release of such data shall be made in a timely manner.
2. The remaining procedures below are not required for CCSBT Members and CNMs to obtain access to data when:
 - The data are listed with a "Low" confidentiality risk classification in Table 1 of the Rules and Procedures for Protection, Access to, and Dissemination of, Data Compiled by the CCSBT; or
 - The data were provided by the Member or CNM seeking access to that data.
3. A written request for access to Non-Public Domain data shall be provided to the Executive Secretary²⁰. In the case of a Member or CNM of the Extended Commission that is seeking access to serve the purpose of the Convention, the Member or CNM shall specify the purpose of the Convention by reference to the relevant article(s). The written request shall use the CCSBT Data Request Form (*Annex 1 to this Attachment*). In addition, the Member or CNM requesting access shall:
 - (a) undertake to only use such data for the purpose described in the written request;
 - (b) complete and sign the CCSBT Data Confidentiality Agreement (*Annex 2 to this Attachment*), and provide the signed agreement to the Executive Secretary; and
 - (c) maintain the requested data in a manner consistent with the CCSBT Data Security Standards specified in **Attachment 1**.
4. For Members or CNMs of the Extended Commission seeking access to data under paragraph 17(c), the Executive Secretary shall forward the completed Data Request Form and the signed confidentiality agreement to the Member or CNM of the Extended Commission that originally provided the data and seek authorisation from that Member or CNM for the CCSBT to release the data.
5. The Executive Secretary shall not authorise the release of more data than is necessary to achieve the purpose described in the written request.
6. The Executive Secretary may attach conditions appropriate for the access to such data (such as that the data be deleted upon achievement of the purpose for which it was released or by a pre-determined date, that a register of persons accessing the data be maintained and furnished to the Extended Commission upon request, etc.)
7. Requests may be made for a standing authorisation, such that Members and CNMs of the Extended Commission may have multiple accesses to the requested data for the same purpose as of the original written request.
8. Dissatisfaction with the Executive Secretary's decisions in regard to access to non-public domain data by Members and CNMs of the Extended Commission shall be resolved by the Chair of the Extended Commission.

²⁰ Requests by Members should be provided only by the Authorised Representative as specified in section 4.4, paragraph 20.

CCSBT Data Request Form

1. Data Requested

The specification of data being requested should refer to the type of data and any parameters relevant to the type of data, which may include, *inter alia*, the gear types, time periods, geographic areas and flags covered, and the level of stratification of each parameter.

[Insert the list of data sets here]

2. Purpose

If non-public domain data are being requested, the use of the data shall be authorised only for the purpose described below.

[If non-public domain data are being requested, insert the description of the purpose for which the data is requested]

3. Persons for whom access to the data is requested if non-public domain data are being requested, the name(s), job title(s) and affiliation(s) of the authorised representative(s) for whom access to the data is being requested shall be listed below; the use of the non-public domain data shall be authorised only for the person(s) listed below.

[Insert the list of persons here]

- Sign the Confidentiality Agreement.

CCSBT Data Confidentiality Agreement

Confidentiality Agreement for the Dissemination of Non-Public Domain Data by the Commission for the Conservation of Southern Bluefin Tuna (CCSBT).

Applicants name(s) and full contact details and signatures

Full name Institution, address and

Contact details

Signature and Date

I/we agree to the following:

- To abide by any conditions attached to use of the data by the Executive Secretary;
- That the data shall be used only for the purpose for which the data are being requested, be accessed only by the individuals listed in Item 3 of the Data Request Form, and be securely destroyed¹⁵ upon completion of the usage for which the data are being requested;
- To make no unauthorised copies of the data requested. If a copy of all, or part, of the data requested is made by the applicant, all copies, or part thereof, will be registered with the Executive Secretary and will be securely destroyed upon completion of purpose for which the data was requested;
- To abide by the CCSBT's Data Security Standards as specified in Attachment 1 of the Rules and Procedures for Protection, Access to, and Dissemination of, Data Compiled by the CCSBT;
- That prior to the publication of any report of an analysis for which the requested data will be used, the report shall be provided to, and cleared by, the Executive Secretary of the CCSBT, who shall ensure that no non-public domain data will be published;
- To provide copies of all published reports of the results of the work undertaken using the data released to the CCSBT Secretariat and to the relevant subsidiary body of CCSBT;
- Applicant(s) will not disclose, divulge, or transfer, either directly or indirectly, the confidential information to any third party without the written consent of the Executive Secretary;
- Applicant(s) shall promptly notify the Executive Secretary, in writing, of any unauthorised, negligent or inadvertent disclosure of confidential information of the CCSBT.
- Applicant(s) assume all liability, if any, in respect of a breach of this Confidentiality Agreement, once the data requested is released to the applicant(s).
- Pursuant to paragraph 25 of the Rules and Procedures for the Protection, Access to, and Dissemination of, Data Compiled by the CCSBT, Member(s) and CNM(s) of the Extended Commission shall not be granted access to non-public domain data until the appropriate actions have been taken to account for any disclosure in violation of the Agreement by the applicant or, *inter alia*, its affiliates, employees, attorneys, accountants, consultants, contractors, or other advisers or agents; and.
- That this Agreement may be terminated by the CCSBT giving written notice to the applicant.