


FFA
**FORUM FISHERIES COMMITTEE
ONE HUNDREDTH AND EIGHTEENTH MEETING**
11-14 May 2021

Agenda Item:	14
Paper No:	FFC118-WP.11
Title:	REVIEW OF THE ISMS POLICY

Summary:

This paper updates the Committee on the review of the application of the ISMS, in particular where it relates to the storage, security and dissemination of personal information. The paper also identifies tasks for the Secretariat to ensure the continual strengthening of the implementation of the ISMS, as well as the need for the possible enhancement of national information security policies and regional information management systems.

Recommendations:

The Committee is invited to:

- i. **Note** the ongoing work in strengthening implementation of the ISMS;
- ii. **Task** the Secretariat to continue work on ISMS, including: (a) ensuring that the relevant international standard is complied with; (b) providing an annual report to the Committee on the operational aspects of the FFA ISMS; and (c) assisting Members in the strengthening of national information security policies; and
- iii. **Task** the Secretariat to explore the possibility of an integrated approach with regards to PNA and FFA information systems and report to the Committee.

1. Introduction

This paper updates the Committee on the review of the application of the ISMS, in particular where it relates to the storage, security and dissemination of personal information. The paper also identifies tasks for the Secretariat to ensure the continual strengthening of the implementation of the ISMS, as well as the need for the possible enhancement of national information security policies and regional information management systems.

2. Background

When considering progress with the Persons of Interest (POI) initiative in 2020, the Committee (FFC114) tasked the Secretariat to review the application of the ISMS, in particular where it relates to the storage, security and dissemination of personal information.

Shortly after FFC114, external consultants were engaged to provide a report to the Secretariat on their review of the implementation of the ISMS. The external reviewers worked closely with the internal ad hoc ISMS working group and submitted their final report to the Secretariat in early 2021. Each of the recommendations of the reviewers was considered by the ISMS Committee and the actions taken are elaborated in this paper.

In March 2021, the MCSWG24: (i) noted the update on the review of the FFA ISMS Policy; and (ii) tasked the Secretariat to provide the annual report to Members on the operational aspects of the FFA ISMS, and to explore the possibility of an integrated approach with regards to PNA and FFA information systems.

3. ISMS Internal Review

The ISMS review report notes that the ISMS covers all information, including personal information, and any generic issues relating to the application and implementation of the ISMS will also be applicable to personal information. Some personal information will be of particular sensitivity, and require high level protection under the ISMS.

The review concludes that the FFA ISMS is itself fit for purpose, and no significant changes are required to its component documents as such, although the usefulness of an additional ISMS policy statement relating to Personal Information was identified. Such a policy statement would highlight the particular sensitivity of some personal information and the need to ensure that it is properly protected.

There are, however, some systematic changes required in the way in which the ISMS is applied and implemented. Of importance is the need to ensure that the ISMS, and information security generally, is properly integrated within the organisation as a whole. ISO Standard 27001, which provides the international benchmark,

emphasises the importance of the information security management system being integrated within an organisation's processes and overall management structure.

The Secretariat is working to address each recommendation identified in the review report. Once the necessary actions have been taken, it would be desirable for FFA to acquire formal ISO certification of the ISMS. This would provide assurance to the organisation and its Members that international best practice has been achieved and is being adhered to including by way of the relevant audit processes.

5. ISMS Committee

The ISMS Committee considered the ISMS review report in detail and made decisions on each of the recommendations made by the reviewers. It is important to note that the Deputy Director-General has overall responsibility for the implementation of the ISMS. An extract of the actions taken by the ISMS Committee for each recommendation is set out in the **Attachment**.

Attachment

EXTRACT OF ISMS COMMITTEE ACTIONS

1. Review of Internal Report Recommendations

The ISMS Committee went through and discussed the 33 recommendations and endorsed them all with the following required actions under each of the recommendations:

1. That the FFA continue, and if possible expand and expedite, its assistance to Members to put in place and implement nationally-developed Information Security frameworks similar in scope to the FFA ISMS (paragraph 14).

The Committee discussed this recommendation and noted that the assistance to Members is ongoing led by Legal and IT. This is work in progress.

2. Once the recommendations in this review have been implemented, FFA should take steps to actively pursue formal ISO certification of the ISMS (paragraph 24).

The Committee noted the importance of implementing the recommendations before pursuing the ISO certification. Work in progress.

3. The Deputy Director-General should be given clear formal responsibility for overseeing the ISMS and ensuring that it is kept up to date and effectively implemented and applied in the future (paragraph 26).

The Committee noted the responsibilities of the DDG, and also noted that this meeting has been convened by the DDG.

4. Consideration should be given to developing an overall Business Continuity Plan, as envisaged in the ISMS, drawing inter alia on lessons learned from the Covid-19 crisis (paragraph 32).

The Committee noted that there is no existing Business Continuity Plan, and the ISMS Working Group (ISMS WG) is tasked in developing this Plan as one of the priorities.

5. The decision should be taken whether or not to proceed with a VMS Policy Statement, and if it is considered necessary the work should be undertaken as quickly as possible (paragraph 35; paragraph 91).

- a. The Committee noted that there are 8 Policy Statements in the ISMS, however, the ISMS Policy Statement 2, provides for the FFA Vessel Monitoring

System and states that it is under consideration noting VMS information is also covered under ISMS Policy Statement 1A, 1B and 8.

The Committee noted that the VMS is also addressed in other policy statements, however, confirmation is to be sought from the VMS Manager of whether or not there is a need to have a standalone VMS Policy Statement.

6. The “Risk Register” should be kept under review, and updated on a regular basis (paragraph 39).

The Internal Auditor has carriage of this task and is responsible for updating on a regular basis. Work in progress and ongoing

7. Consideration be given to holding a further Workshop on Risk Assessment, and the workshop’s outcomes should be reviewed by management on a regular basis (at least once a year) to determine whether further updating may be required (paragraph 40).

The last workshop was held on 24 and 30 January 2014 respectively. The Committee noted this recommendation and there are plans for another workshop.

8. The requirements and standards of data sharing arrangements should be subject to regular review (paragraph 41).

The committee discussed this recommendation noting that there is a paper for the MCSWG24 for the establishment of a list of data to be shared. Also noting that the ISMS WG is working on the data classification.

Data sharing work is work in progress. The ISMS WG is working on the data classification and will report back to the Committee.

9. The use of a standard Non-Disclosure Agreement (NDA) should be considered for consultants and contractors, to supplement the language found in the standard contract for non-disclosure of confidential information (paragraph 42).

This is work in progress. The ISMS WG has a draft NDA to be further considered by the WG.

10. Consideration should be given to whether there are sufficiently adequate remedies for any breaches of the obligations under the ISMS (paragraph 43).

FORUM FISHERIES COMMITTEE EYES ONLY

The Committee noted that with regards to the remedies for breach of the ISMS by FFA employees, there may be sufficient remedies as provided in the ISMS, however, there are concerns with regards to breaches by other users. The use of the NDA may address this gap.

This is work in progress. The draft NDA considered by the ISMS WG should ensure that remedies are sufficiently adequate to address the breaches of the ISMS by users, consultants and contractors.

11. A system should be established to identify how regularly aspects of the ISMS stipulated as requiring review actually need to be reviewed, and then a diary (i.e. reminder) system should be set up to ensure that this happens (paragraph 44).

The Committee tasked the ISMS WG to keep track of provisions of the ISMS that require review and to set up a system for such.

12. A formal Register for the recording for all breaches of information security, actual or suspected, should be established as required by the ISMS (paragraph 45).

The Committee discussed who is the Registrar of breaches of Information security. This should be put as a standing agenda for the ISMS Committee Meeting, and the committee to decide on who should be the custodian of this register, and there may be a need to consider the investigation of any breach.

13. A comprehensive training and awareness programme should be developed on the ISMS and information security. This should be part of the initial training of new employees, tailored according to their positions. Refreshers should also be provided for staff, and all staff should be updated when there are changes to the ISMS itself. Interactive training materials should be developed for this purpose. A check-sheet type process should be used to ensure that staff, and training, do not slip through the cracks (paragraph 48; paragraph 95; paragraph 96).

The Committee agreed to progress the training for staff, and this may form part of the orientation and induction programme. The Committee recommended that the Training Advisor should consider this as part of FFA's programme for orientation and induction.

14. The archiving practice should be reviewed, including its application to personal information, and it should be formalised in an appropriate Policy Statement (paragraph 49).

FORUM FISHERIES COMMITTEE EYES ONLY

The Committee members expressed their concerns on the archiving practice, noting that bundles and boxes of documents are lying everywhere on and under desks. Beside the security issues, this also creates fire hazards.

The Committee agreed to formalise a policy Statement to address this issue as a priority. The Corporate Services Division is tasked to carry out the survey on the amount of documents in the office. A policy Statement is to be developed and reviewed in the next meeting.

15. The ISMS Committee should resume its regular meetings in accordance with its ToR as a matter of priority, and fully undertake all of the responsibilities in its ToR (paragraph 54).

The Committee is committed to its quarterly meetings, and agreed to lock in the schedule for quarterly meetings. The next meeting of the ISMS Committee will be before the FFC, and then quarterly meetings will be locked in afterward.

16. The ToR of the ISMS Committee should be internally reviewed for updating as is required at least every two years (paragraph 55).

The Committee agreed to undertake the review of the ToR every 2 years.

17. The Security Custodians should carry out regular scheduled reviews relating to the designated systems and information assets for which they are responsible (paragraph 66).

18. Security Custodian responsibilities should be formally included in the job descriptions for the relevant managerial positions (paragraph 67).

Both recommendations 17 and 18 were considered together as they are both similar. The Committee agreed that the Security custodian responsibilities should be set out in their job description. HR is tasked to implement this.

19. Internal organizational data classification should be pursued at the departmental level to comply with the ISMS Policy (paragraph 68; paragraph 85).

This is work in progress. The ISMS WG is working on the classification of data and to report back to the Committee.

20. The list of Security Custodians and related systems or information assets should be regularly reviewed and updated so as to ensure that it is up to date and complete (paragraph 69).

The Committee noted the need for a regular review and update of the list of Security custodians, and tasked the Strategic Communications Manager for internal communication and awareness of such updated list of security custodians.

21. A whole of organization approach should be developed as a matter of priority, to communicate the organisation's security policies to all employees, contractors and third parties to ensure that they clearly understand their responsibilities (paragraph 70).

HR is tasked to ensure that this recommendation is implemented.

22. Security responsibilities should be included in job descriptions as a matter of priority (paragraph 71).

The Committee agreed with this recommendation and tasked HR to implement.

23. The Access Control Policy, which is in draft, should be finalised and formalized as soon as possible (paragraph 73).

The Committee noted that this draft policy was discussed in the ISMS WG and the WG made recommendation for its adoption.

The Committee agreed to revisit this matter in the next meeting for approval and adoption.

24. The Incident Response Procedure, which is in draft, should be finalised and formalized as soon as possible (paragraph 78).

The Committee noted the review and recommendation made by the ISMS WG for adoption of the draft Incident response procedure. To be considered and adopted in the next meeting

25. Any necessary work should be completed as soon as possible to ensure that staff are bound by the confidentiality agreement for Data Users (paragraph 82).

The Committee tasked the HR to implement this by having staff sign the form and to be part of the attachment to existing employment contract.

26. Consideration of a Data Leak Procedure should be expedited (paragraph 83).

The Committee noted this is work in progress as the ISMS WG has a draft to progress.

27. Work should be taken forward on the draft FFA Information Security Policy, for further consideration and if appropriate approval (paragraph 86).

The Committee noted and discussed whether this might be covered under the cyber security policy. The IT Manager is tasked to compile a list as to which FFA information security policies are current and which are redundant, and to provide further clarifications.

28. Verification checks should be carried out on all new employees as required by the ISMS (paragraph 92).

The Committee tasked the HR to develop a process and checklist for a background check of any new employees.

29. A warning system should be developed to clearly identify the classification of sensitive materials when being viewed on screen, or when printed. This should apply not only when classified information is being viewed by FFA staff, but also when it is being viewed in Member countries (paragraph 99).

The Committee noted that the Secretariat is behind in this area and therefore this matter is classified as high priority. The Committee noted the work on the classification of data carried out by the ISMS WG. The committee agreed that there should also be training to Staff on this matter.

30. The Secretariat should review the handling of sensitive and classified information, particularly the implementation of a clear desk requirement, the requirement not to leave computers vulnerable when unattended, the use of shared printers, and the disposal of sensitive and classified information (paragraph 102).

The Committee endorsed this and noted the volume of papers lying around, and agreed that there should be a review of how documents are being handled, including photocopying and the use of shredders. This is classified as high priority. The Corporate Services Division is tasked with addressing this.

31. The draft Incident Response Plan should be finalised and formalized as soon as possible (paragraph 105).

The Committee agreed to have this draft reviewed and to be considered in the next meeting, and tasked the IT Manager to report back to the Committee.

32. Further consideration should be given to the statement “It is acknowledged that no RQSP is bound by the guidelines set out in this policy statement”, contained in ISMS Policy Statement 8 (paragraph 111)

The Committee noted the statement in the ISMS and agreed to review the language to provide that RQSP are also bound by the guidelines as set out in the ISMS.

33. The Secretariat should consider developing a new ISMS Policy Statement on “Personal Information” (paragraph 132).

The Committee tasked the ISMS WG to develop a new ISMS Policy Statement on personal information including in relation to POI.

2. Recommendations to adopt ICT policies

There were four draft policies and procedures that were recommended by the ISMS WG:

- i. the Acceptable Use policy;
- i. the Internet Acceptable use policy;
- ii. the Network Security policy; and
- iii. the Procedure to secure published FFA meeting papers on the FFA website.

The Committee only approved and adopted the Acceptable Use Policy (AUP), and agreed that the AUP must be implemented by Staff. The approach agreed is for the Director General to send a circular to advise all staff on the policy and its implementation.

3. Any Other Matters

There was a concern raised as to the security on sharing of sensitive meeting documents as google documents. IT Manager to provide advice.

The Committee agreed to have the next meeting sometime before the FFC and a quarterly meeting shall be scheduled thereafter.