Pacific Islands Forum Fisheries Agency (FFA)

Information Security Management System

Document Details

Author:	Consultant
Version:	2.1
Document Status:	Approved FFC110

Security classification	**Open**		
Date of review of security classification			
Authority	ISMS Committee		
Author	Consultant		
Documentation status	Working draft	Consultation release	☑ Final version

TABLE OF CONTENTS

1. Introduction

Information is an asset that FFA has a duty and responsibility to protect. The availability of complete and accurate information is essential to FFA functioning in an efficient manner to provide products and services in support of effective fisheries management.

The organisation holds and processes confidential and personal information on private individuals, employees, partners and suppliers and information relating to its own operation. In processing information FFA has a responsibility to safeguard information and prevent its misuse.

The objective of the FFA Information Security Management System (ISMS) is to ensure that its core and supporting activities continue to operate with minimal disruptions.

The purpose of FFA's ISMS is to set out a framework for the protection of the organisation's information assets:

- From all threats, whether internal or external, deliberate or accidental;
- To enable secure information sharing;
- To encourage consistent and professional use of information;
- To ensure that everyone is clear about their roles in using and protecting information;
- To ensure business continuity and minimise business damage; and
- To protect the organisation from legal liability and the inappropriate use of information.

The ISMS is a high level document and sets out a number of controls to protect information. The controls include Policy Statements, processes, roles and responsibilities. The ISMS must be read in conjunction with several other FFA policy documents, including the Staff Regulations, FFA ICT Manual and FFA Business Continuity Plan.

2. Scope

The ISMS outlines the framework for management of Information Security within FFA.

The ISMS applies to all staff and employees of FFA and contractual third parties and agents of FFA who have access to FFA's information systems or information.

The protections assigned to *shared* data held within FFA information systems apply to use, storage and protection of that data even when held at the national level. FFA members are required to implement nationally-developed Information Security frameworks similar in scope to the FFA ISMS.

The ISMS applies to all forms of information including:

- Speech, spoken face to face, or communicated by phone or other means such as VOIP;
- Hard copy data printed or written on paper;
- Information stored in manual filing systems;
- Communications sent by post / courier, fax, electronic mail;

- Data stored and processed via servers, PC's, laptops, mobile phones, PDA's; and
- Data stored on any type of removable media, CD's, DVD's, tape, USB memory sticks, digital cameras.

3. Structure of the ISMS

The ISMS is based upon ISO 27001 the International Standards for Information Security and is structured to include the main security category areas within these standards. FFA's intention is to continually strengthen the ISMS with the goal of attaining formal certification under the ISO.

The ISMS is a high level policy document supplemented and extendable by:

- additional Policy Statements which provide detailed policies and guidelines relating to specific security controls. A schedule of Policy Statements is Annexed to the ISMS and will be updated from time to time as part of FFA's ongoing security risk management process; and
- cross references to other FFA policy documents that have a bearing on achieving the scope, purpose and objectives of the ISMS as outlined above.

The structure provides an efficient management context that allows FFA to adapt to changes in information security requirements and standards.

4. Risk Management

Information security requires the management of risk from physical, human and technology related threats associated with all forms of information within or used by the organisation.

FFA policy is to ensure that information is secured against three information security risk management criteria of confidentiality, integrity and availability.

FFA's standard business practice will be to continually assess information security risks against the following domains of security:

- Computer system security: CPU, Peripherals, and OS. This includes data security.
- Physical security: The IT equipment and premises dedicated to the housing of IT Equipment.
- Operational security: Environment control, power equipment, and operation activities.
- Procedural security: Outlined by IT, vendor, and management personnel, as well as Authorised Users.
- Communications security: Communications equipment, personnel, transmission paths, and adjacent areas.
- Application security: To include access, authentication and authorisation.

Information security risks may arise or be associated with Individual security awareness; user access levels and logging facilities; backup and disaster recovery mechanisms; protection from viruses and other malware; existence of exploitable software deficiencies; intercept and capture of FFA data in transit; system compromise through overuse and denial of service; controls over changes made to systems and/or data; and sabotage and intrusion.

5. Organisation of Information Security

5.1. Statement of Management Intent

It is the policy of FFA to ensure that information will be protected from a loss of:

- Confidentiality, information is accessible only to authorised individuals.
- Integrity, safeguarding the accuracy and completeness of information and processing methods.
- Availability, authorised users have access to relevant information when required.

Requirements and standards of data sharing arrangements, contractual or otherwise, are incorporated in the ISMS and will be subject to review and extension on an as needs basis.

All breaches of information security, actual or suspected, must be reported to the Deputy Director-General. Such reports will be recorded in a register and will be investigated.

Business continuity plans will be produced, maintained and tested.

Information security education and training will be made available to all staff and employees.
Information stored by the organisation will be appropriate to the business requirements.

5.2. Information Security Coordination

The Secretariat has established a functioning ISMS Committee (TOR attached) to oversight the ISMS and make recommendations on improving and enhancing related to, *inter alia*, ISMS Policy Statements, related or referenced FFA policy documents, procedures, incident management and security management awareness.

The ISMS Committee will assess if the ISMS enables the FFA community to maintain an acceptable risk treatment for information security risks and will make recommendations with the respect to development, review and implementation of polices to assist Authorised Users and System Custodians to meet their information security responsibilities.

Amendment and Evolution of Information Security

The ISMS is administered by the FFA Secretariat. The Director-General may approve editorial or minor procedural amendments to the ISMS based on recommendations of the ISMS Committee or the Monitoring, Control and Surveillance Working Group (MCSWG). Any such amendments must be notified to the MCSWG.

Substantive changes to the ISMS or its Policy Statements, particularly changes that impact on the way that data or information owned by FFA members (individually or collectively) is used and shared must be approved by FFC.

Changes to cross-referenced FFA policy documents will be approved by the Director-General as long as they do not materially change the application of the ISMS.

The Secretariat will ensure that the most current version of the ISMS and any cross referenced FFA policy documents are available on the FFA website.

5.3. Information Security Responsibilities

Individuals

All staff and employees of the organisation, contractual third parties and agents of the organisation, and any other Data User (as defined in Policy Statement 1A below) accessing FFA information are required to adhere to the ISMS, processes and procedures.

For the purposes of the ISMS, any reference to staff or employees of FFA applies equally to the employee of any other organisation that is based and works within FFA in accordance with the FFA Annual Work Plan and Budget.

Users of FFA Information shall:

- Preserve security and privacy of systems and the information contained within them in accordance with the ISMS.
- Report known, likely, and any suspected security breaches to the Deputy Director-General.
- Make themselves aware of their responsibilities for Information Security and discharge their ISMS obligations accordingly.

It is a condition of employment with the Pacific Islands Forum Fisheries Agency that a staff member shall not communicate to any person, organisation, government or to the press any unpublished information known to them by reason of their official position without obtaining prior permission of the Director-General. This applies at all times during and after termination of employment.

Failure by a staff member to comply with the ISMS and its processes and procedures will lead to disciplinary and remedial action. The FFA Staff Regulations (link) provide the basis for such disciplinary action, but it should be noted that some additional remedies, such as restricted access to data may be considered by the Director-General if appropriate.

Division Directors

Through their membership of the ISMS Committee, and in discharging their management duties for their own divisions, Division Directors and the Deputy Director-General are responsible for ensuring:

- The Information Security policy is implemented and adhered to within their respective business units;
- That all staff and employees, contractual third parties and agents of the organisation are made aware of and comply with the ISMS;
- That appropriate data access privileges are provided for staff members within their Division.

Security Custodians

Security Custodians hold responsibilities for designated systems and information assets with authority to make decisions related to the development, maintenance, operation of applications and associated data consistent with the ISMS. Responsibilities include:

- Reviewing data classification and sharing requirements for the designated system and, if necessary recommending appropriate changes to the ISMS Committee;
- Reviewing access rights and privileges of existing approved users and reviewing and actioning new user requests;
- Establishing measures to ensure data integrity for access to data (including data backups);
- Developing a business continuity and disaster recovery plan in case of system failure;
- Reviewing usage information; and

Security Custodians are specified below and may be updated from time to time by the Director-General on advice from the ISMS Committee:

System or information asset	**Security Custodian:**
FFA Secretariat system platforms (e.g. servers):	IT Manager
FFA Secretariat communications systems:	IT Manager
FFA Secretariat managed computing facilities:	IT Manager
FFA VMS Systems:	VMS Manager
FFA Register of Good Standing Vessels:	VMS Manager
FFA Observer Systems:	Observer Manager
FFA RFSC Data:	Director, Fisheries Operations
Corporate Finance Applications:	Finance Manager

6. Asset Management

FFA's assets will be appropriately protected.

All assets (data, information, software, computer and communication equipment) will be accounted for and have an owner.

In the case of physical assets, ownership will be assigned and monitored through the FFA Asset Register (link). In the case of data and information stored on FFA computers and network drives, the Director-General will be the owner.

7. Human Resource Security

The organisation's security policies will be communicated to all employees, contractors and third parties to ensure they understand their responsibilities.

Security responsibilities will be included in job descriptions and in terms and conditions of employment.

Further policy intentions and procedures are outlined in Policy Statement 3.

8. Physical and Environmental Security

Classified (non-public domain) information processing facilities will be housed in secure areas protected by defined security perimeters with appropriate security barriers and entry controls (see Policy Statement 1B).

Classified (non-public domain) information will be physically protected from unauthorised access, damage and interference (Policy Statements 1A and 1B).

9. Communication and Operations Management

FFA has and will operate its information processing facilities securely.

Procedures for the management, operation and ongoing security and availability of all data and information processing facilities are contained within specific ISMS Statements.

10. Access Control

Within the FFA ISMS construct, information is classified not Data Users. Access to FFA information and information systems is made available to all staff unless a specific case is made by Executive Management or a Division Director for increased protection. The final decision for access to FFA information and information systems, and any subsequent decisions regarding access to specific FFA information and information systems shall be made by Security Custodians, in consultation with the Director General where necessary.

Access will be granted or arrangements made for employees, partners and suppliers according to their role, and only to a level that will allow them to carry out their duties.

A formal user registration and de-registration procedure will be implemented for access to all information systems and services. These procedures will be developed by each security custodian and considered by the ISMS Committee. Procedures will be based on the following principles:

- For FFA staff – a specific case must be made by the Division Director for their staff to gain access to a systems or data that is not generally open;
- Similarly, for contractors – the FFA contact specified in the contract must make a specific case;
- For FFA members – requests for access to given systems or data must be lodged by the Official Contact for the FFA member; and
- Where the security custodian is aware that a Data User has left the Secretariat, completed a contract or left employment with an FFA member, they will be removed.

The Secretariat will establish an online, publicly available register of data users for each system or data type held by FFA. Members will be responsible for regularly reviewing and, if necessary requesting updates to the register through their Official Contact. Requests for updates will be a standing agenda item for the MCSWG.

11. Information Systems Acquisition, Development, Maintenance

Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems.

Risk assessments with controls to mitigate risks will be implemented where appropriate.

12. Information Security Incident Management

All users are responsible for communicating information security incidents, known or suspected, as well as any potential vulnerabilities associated with information systems as soon as practicable to the FFA IT Helpdesk (email helpdesk@ffa.int or phone +677 7425263). The Helpdesk will log the incident and advise the Deputy Director-General immediately.

Under direction of the Deputy Director-General, the IT Manager and relevant Security Custodian and, if applicable, relevant Division Director(s) will assess the incident or vulnerability controls in place and make an escalation determination for notifying the Director General and ISMS Committee. Escalation to this level will generally occur where the incident poses an information security risk to FFA.

13. Business Continuity Management

FFA will have in place arrangements to protect critical business processes from the effects of major failures or breaches of information systems or disasters and to ensure their timely resumption. The FFA Business Continuity Pan is available at (link).

14. Compliance

FFA will ensure that any statutory and regulatory law or contractual obligations affecting its information systems are upheld by the ISMS. The design, operation, use and management of information systems will comply with all legal, regulatory and contractual security requirements.

Annex 1: Definitions

Term	Definition
Administration	Tasks (including testing and scanning) undertaken by IT Services Authorised Staff to ensure maintenance of security of IT services and systems within the FFA domain.
Asset	Anything that has value to the organisation
Authorised User	Any user who has been authorised by the relevant officer to access a system or IT facility, and includes (but is not limited to) staff of FFA, staff of member countries fisheries management authorities, or any company in which FFA is pursuing a collaboration such as consultants, recognised visitors, etc.
Availability	Availability refers to the ongoing operations and delivery of intended services by a system (e.g. finance or payroll) and its components.
Control	Means of managing risk, including policies, procedures, guidelines, practices
Confidentiality	Confidentiality refers to the need to ensure that information is accessible only to those authorised to have access.
Guideline	A description that clarifies what should be done and how
Information Security	Preservation of confidentiality, integrity and availability of information
IT Authorised Staff	FFA staff authorised by the IT Manager to monitor accounts, files, stored data and/or network data, and to disconnect IT equipment in the event of an Information Security breach.
IT Services	Information and Technology Services
Integrity	Integrity refers to the accuracy or correctness of data. Loss of data integrity may be gross and evident, as when a computer disc fails, or subtle, as when a character in a file is altered
Policy	Overall intention and direction as formally expressed by management
Privacy	The restriction of access and appropriate use of personal information.
Public Information	Information that, from time to time, is available for general access without the requirement for authentication.
Security	The state of being free from unacceptable risk.
System Custodian	The person authorised as responsible for a system and/or its information content. See section 4.3 Information Security Responsibilities above.
Threat	The potential cause(s) of losses or damage. These may include human or non-human, natural, accidental, or deliberate.

Annex 2 – Terms of Reference of the FFA ISMS Committee

Background

At its Eighty-First Meeting of the Forum Fisheries Committee (FFC81) in Nuku'alofa, Tonga, the Committee endorsed the draft FFA Information Security Management System (ISMS) following the recommendations of the Fifteenth Meeting of the Monitoring, Control, and Surveillance Working Group (MCSWG15).

The FFA ISMS specifies an "*FFA Security Committee*" comprising of Division Directors to "*oversight the ISMS and make recommendations on improving and enhancing the ISMS related to, but not inclusive of, Policy Statements, procedures, incident management and security management awareness.*"
This committee was formally established as the *FFA ISMS Committee* and held its first meeting on November 25, 2016[i].

Terms of Reference

Membership

1. Members of the ISMS Committee will be as follows:
    a) Director-General (DG)
    b) Deputy Director-General (DDG)
    c) Director Corporate Services (DCS)
    d) Director Fisheries Development (DFD)
    e) Director Fisheries Management (DFM)
    f) Director Fisheries Operations (DFO)
    g) Internal Auditor (IA)
    h) Legal Counsel (LC)
    i) Manager IT (MIT)
    j) Manager Finance (MFIN)
    k) Secretary (nominated by the Committee)

2. The DG, or designate, will be the Chairman of the ISMS Committee.

3. Other technical staff may be invited to meetings of the ISMS Committee depending on the agenda.

Secretary

4. A Secretary may be nominated by the ISMS Committee and will be responsible for recording, circulating, finalising and storing appropriately the Minutes of the meeting.

Reporting

5. The ISMS Committee will report to FFC as required, either in the form of a separate paper where warranted or as part of a relevant related paper such as on Monitoring, Control and Surveillance. Matters requiring FFC attention or decision will be put forward to FFC with appropriate recommendations for consideration.

Notice/Frequency of Meetings

6. The ISMS Committee will meet on a quarterly basis throughout the year or more frequently as circumstances dictate.

7. In consultation with the DDG, the DCS will be responsible for calling ISMS Committee meetings and together with the Secretary will coordinate an agenda and any papers for the meetings.

Responsibilities

8. The ISMS Committee will be responsible for:
   a) Ensuring the ISMS is implemented and the security objectives of the FFA ISMS are met;
   b) Oversight of the implementation and operation of, and compliance with, the FFA ISMS including making recommendations on improving and enhancing the FFA ISMS relating to Policy Statements, IT hardware and software, procedures, incident management and security management awareness;
   c) Considering any issues of information security including reported and potential ICT-related security threats and incidents;
   d) Ensure the FFA's Business Continuity Plan (BCP) is up-to-date and promulgated and consider its activation following any catastrophic events impacting on the integrity of the Secretariat's normal business processes;
   e) Developing an annual work plan to maintain and improve information security within the Secretariat;
   f) Considering related outcomes from other relevant security groups such as the FFA Security Committee, QUADs and through CROP processes; and
   g) Reviewing the status of Member Country adoption of national ISMS policies, consider any requests for assistance arising from such reviews, and advising the FFC of any implications for members regionally arising from such work at the national level.

Information Requirements

9. The following information will be provided to meetings of the ISMS Committee:
   a) Status report on FFA ISMS implementation including metrics on staff and employee awareness training, data access requests, etc.
   b) Metrics on suspected and reported information security breaches;
   c) Report on the mandatory testing of the FFA ICT Business Continuity Plan (BCP) including on respect of disaster recovery procedures;
   d) Status report of progress against the annual work plan; and
   e) Status report of Member country information security policy implementation.

Updating the Terms of Reference

10. Noting the pace of change within the IT sector, these Terms of Reference will be updated by the ISMS Committee at least every two years.

    Last Update: April 2019.

Schedule of Information Security Statements

ISMS Policy Statement 1A:	Data Access and Use
ISMS Policy Statement 1B:	MCS Regional Information Management Facility
ISMS Policy Statement 2:	FFA Vessel Monitoring System (under consideration noting VMS information also covered under ISMS Policy Statements 1A, 1B and 8).
ISMS Policy Statement 3:	Human Resource Security
ISMS Policy Statement 4:	Appropriate Use of Email
ISMS Policy Statement 5:	Information Backup
ISMS Policy Statement 6:	Infrastructure Hardening
ISMS Policy Statement 7:	Appropriate Use of Internet
ISMS Policy Statement 8:	Arrangements for sharing of data and information between FFA Members, FFA Secretariat and Recognised Quadrilateral Surveillance Providers

**ISMS Policy Statement 1A:		Data Access and Use**

Document Details

Author:		Fisheries Operations Division
Version:		1.0
Document Status:	Approved FFC110

Security classification	**Open**		
Date of review of security classification			
Authority	Director of Fisheries Operations		
Author	MCS Specialist		
Documentation status	☑ Working draft	Consultation release	Final version

1. Purpose

ISMS Policy Statement – Data Access and Use defines FFA policy concerning classification and access to information held on behalf of the FFA members within FFA Data Resources. It provides guidelines and requirements for:

- confidentiality classification of FFA data and information; and
- access and use of FFA data and information.

Notes:

- *ISMS Policy Statement 1B – FFA MCS Regional Information Management Facility (RIMF)* conjuncts with this policy and provides further security control regarding information within and distributed from the FFA MCS RIMF.
- *ISMS Policy Statement 8 – Arrangements for sharing of data and information between FFA Members, FFA Secretariat and Recognised Quadrilateral Surveillance Providers* also provides additional guidance on specific data sharing arrangements with surveillance providers.
- The FFA Small-Scale Foreign Fishing Vessel Strategy as adopted by FFC104 encourages the sharing of relevant data with non-FFA member countries effected by illegal small foreign vessels (notably New Caledonia).
- The *Agreement on Strengthening Implementation of the Niue Treaty on Cooperation in Fisheries Surveillance and Law Enforcement in the South Pacific Region* (NTSA) contains certain provisions for minimum data sharing between Parties to that Agreement and these are referenced below.

2. Scope

The scope of the *ISMS Policy Statement – Data Access and Use* is information held within FFA Data Resources. It applies to all Data Users and deals with individual responsibilities for ensuring the correct classification and distribution of data that accounts to the rights of Data Owners and the privileges of Data Users.

Data Owners

FFA Data Resources consist of different types of data provided by various sources. These data sources are considered to be the ‘owners’ of the data provided and they can authorise, or revoke authorisation, regarding the use of their data. For the most part, the ownership of data is at a member level; that is, a specific set of data is deemed to be owned by the particular member that provided it.

Data Users

Data and information held within FFA Data Resources can be accessed and used by a number of 'data users'. A Data User is defined as an individual or organisation authorised in accordance with these rules and procedures to access and make use of data and information for a defined legitimate purpose. Data Users can make use of data owned by different owners as authorised by the owner at any specific point in time. Access to data may vary among users.

3. Risks

Confidentiality (risk) of FFA Information Resources with respect to data access and usage is managed using a 'traffic light protocol'. Refer to *Table 1: Classification Guidelines*. This protocol provides flexibility to accommodate pre-existing and future data dissemination authorisations by employing four colours to indicate (1) different degrees of sensitivity, (2) the corresponding sharing considerations to be applied by the recipient(s), and (3) what further dissemination, if any, can be undertaken by the recipient.

4. FFA Policy

Data Owners and Data Users providing, using and distributing data will apply the Classification Guidelines set out in Table 1 *Information Security Classification Guidelines,* with the following procedures and rules:

- Data may only be accessed if the Data Owner providing the data to FFA Data Resources authorises its release. In the case where there is no individual owner, data will be accessed according to the rules applicable to the confidentiality classification of such data.
- "Data Owners may authorise the release and dissemination of data by:
  - Specific authorisation (using the template set out in Annex A), or
  - Authorisation under an international agreement or arrangement[1]
- Data Owners can selectively authorise access to and use of the data they own. This can be reflected in two ways. Owners may:
  - authorise certain data types but not other data types; or
  - give authorisation for access to certain Data Users but not to other users.
- Any Data Users who are authorised to access a Data Owner's data must agree to be bound by the confidentiality agreement in Annex B
- Data Users cannot disseminate information they are authorised to access to another party unless such party is also an authorised as a data user of the same data by the data owner.
- If the classification for a particular data type cannot be easily and readily determined, then either a higher level should be assigned, or the data type

[1] For example, under Article 19 of the NTSA, Parties, by virtue of being Parties to that Agreement, have authorised the sharing of fisheries data and intelligence (as defined in that Agreement) with all other Parties for fisheries purposes.

should be broken into two or more data types for which classification can be readily assigned.

- Information for dissemination will be labelled with the correct Classification code, usually by including “[Classification Code] - [Colour]” in unambiguous text in the header and footer of the document. In the event that information needs to be shared more widely than indicated by the original designation, the request must be referred back to the Data Owner.

- Where information for dissemination also includes protected data from another source (such as WCPFC non-public domain information), it shall be assigned a suitably high classification to ensure that information is not disseminated to users that do not have access to it through other means.

- Multi-user IT systems will have the allocation of privileges controlled through a formal authorisation process. Privileges will not be granted until the authorisation process is complete, a record of all privileges allocated will be maintained in the register described in section 10 of the ISMS.

- Employees of multilateral organisations with common membership and a history of cooperation with FFA members and the FFA Secretariat may be granted ongoing access to classified information that is in the form of FFC working papers, FFA briefs and the associated discussions. This will be considered on a case by case basis by the Director-General and will be facilitated by written agreement at the organisation level that such employees will treat such information appropriately. Written agreements will include reciprocity.

- Official observers to FFC will be granted access to information and working papers based on a case by case assessment of the confidentiality, strategic importance and sensitivity of the issues. The Director-General or Deputy Director-General will decide whether to restrict access to observers. Where there is doubt, access will be restricted and the question put to the relevant meeting.

Provision of reports containing classified information for donor reporting and monitoring and evaluation purposes

It is FFA policy to provide reporting and M&E data that is as complete and transparent as possible to ensure that all stakeholders, including donors, have as full an appreciation as possible of the work that has been undertaken and the cogent findings or outcomes. However, <u>that policy intent does not in any way override or supersede the provisions, procedures or rules of this ISMS.</u> Where reports or M&E data would contain or reveal classified information, the same rules of data ownership and authorisation shall apply. Donors and other stakeholders should not have any expectation to access classified information on the basis that they have funded or otherwise contributed to work.

5. Compliance

If any FFA employee is found to have breached this Information Security Policy, they may be subject to Disciplinary action as per section 5.3 of the ISMS.

Any violation of the policy by a temporary worker, contractor or supplier may result in the termination of their contract or assignment or other relevant legal action relating to breach of contract.

Any violation of the policy by a Data User other than an FFA employee or contractor may result in suspension of data access privileges for a period of time as determined by the relevant data owner and, in extreme cases, FFC.

Table 1: Information Security Classification Guidelines

When should it be used?	Classification	How Should it be shared?	E.g. Information / Data Types (regardless of how it is provided or how authorisation to share is given by the data owner)
When information cannot be effectively acted upon by additional parties, and could lead to impacts on a member's privacy, reputation, or operations if misused.	Classified High - RED	Recipient may not share the information, unless specific authorisation is granted by the data owner in accordance with the rules above. Internet exchanges will use at a minimum Hypertext Transfer Protocol Secure (HTTPS), with individual user accounts for web based portals or email exchange The Secretariat will continue to actively test and trial additional protection and encryption mechanisms for RED and YELLOW information or data such as third party and/or two-factor authentication and additional protocols such as HSTS HTTP.	Operational level catch and effort data Access Agreements MCS compliance analysis and profiling for deriving risk levels of: ○ Persons of interest ○ Vessels compliance risk[2] Financial information, access agreements and other data specific to the administration of a specific fund or fishery at the national level. Name and address details of observers.
When information requires collaborative and cooperative support to be effectively acted upon, but carries risk to privacy, reputation, or operations, if shared outside of FFA.	Classified Medium - YELLOW	May be shared with participating members and Surveillance Provider where dissemination of information needs to be tightly controlled. Internet exchanges will use at a minimum Hypertext Transfer Protocol Secure (HTTPS).	MCS Compliance index for: ○ persons of interest ○ vessels of interest (the Google earth surveillance picture) Real time or historic location, activities and movement of fishing vessels including VMS data and the Regional

[2] The RFSC assigns each vessel listed on the FFA Record of Good Standing within the RIMF a compliance index. The underlying analysis used to assign an index draws on classified and open source material. The first pass analysis focuses on:

- Negative Correlations between data holdings of VMS, Observers, and Vessel Reporting Requirements;
- Geographical location of the vessel in, or within, close proximity of an EEZ in which it does not hold a fishing license;
- At-sea and in-port Inspection reports;
- Aerial surveillance information; and
- Monitoring RFMO IUU lists

			Surveillance Picture FFA RFV – all details Individual observer reports or unaggregated observer data. Planning documents for Regional Surveillance Operations where the official is from an FFA Member country or a Surveillance Provider participating in the operation. Commercially sensitive information such as financial accounts, cost benefit analyses of development proposals, and due diligence assessments of specific entities. Current licence lists
When information is useful for the awareness of all FFA members.	Classified Low - GREEN	May be shared with FFA members but is not to be shared in public forums. May be shared with FFC Observers but only after specific review and decision by the Director-General or Deputy Director-General	FFC and subcommittee papers and briefings e.g. Management Options W/S, MCS WG, FFA Pre-WCPFC meetings. Catch and Effort, including observer data which has the following resolution: * Longline 5°x5°/month and all flags combined * Purse seine 1°x1°/month and all flags combined Historic licence lists
	Unclassified Open - WHITE	Public domain data – information may be shared freely, may be made freely available, and is subject to standard copyright law.	WCPFC Vessel Register RFV vessel details – name, flag, call sigh, FFA ID Specific details on all fully adjudicated prosecutions, violations and settlements relating to fishing vessels that are a matter of public record.

Annex A: FFA MCS INFORMATION ACCESS AUTHORISATION

Data held in FFA Data Resources and authorised for use by the Data Owner shall only be accessed and used in accordance with the 'FFA Information Security Policy'.

Data Owner

Name (Organisation / Institution)	Of Country (N/A if IGO)

Data User

Name (Organisation / Institution)	Of Country (N/A if IGO)
E.g. FFA RFSC	
E.g. FFA Authorised MCS Persons	

The Data Owner agrees to provide to the Data User access to the following Data Types with the specified classification.

Data Type	Data Classification
E.g. Licensing data, VMS data, log book data	
E.g. VMS data	
E.g. Log book data	

Additional Terms of Authorisation

Name: ....
Position ....
Email: .... Signature: ....
Organisation: ....
Date: ....

Annex B: FFA DATA USERS CONFIDENTALITY AGREEMENT

Data User

Name (Organisation / Institution / Surveillance Operation)	From Country (or ‘multi-country’)

Purpose and details of the data to be used

Purpose of the data requested	Details of the Data Requested

Representatives to be authorised

Full name	Contact Details	Signature and Date

I/we agree to the following:

- That the data shall be used only for the purpose for which the data are being requested and be accessed only by the individuals listed as Data User’s representatives listed on this DCA Form;
- To make no unauthorised copies of the data requested;
- To destroy the data being provided, including any authorised copies made, upon completion of the usage for which the data are being requested if directed so by the Data Owner;
- To abide by standards no less stringent that the FFA Information Security Management System;
- That publication, outside the community of authorised Data Users, of any report that includes data and information provided, requires the prior approval of FFA’s Director General and the Data Owner(s);
- Will not disclose, divulge, or transfer, either directly or indirectly to any third party, the data provided to them by the FFA;
- The Data User representatives listed on this Confidentiality Agreement Form shall promptly notify the FFA Director General, in writing, of any unauthorised, negligent or inadvertent disclosure of data provided to them by FFA;
- Data User’s representatives listed on this DCA Form assume all liability, if any, in respect of a breach of this Confidentiality Agreement, once the data requested is released to a representative.

This Agreement may be terminated by giving written notice to the other party.

ISMS Policy Statement 1B: MCS Regional Information Management Facility

Document Details

Author:	Fisheries Operations Division
Version:	1.0
Document Status:	Approved FFC110

Security classification	**Unclassified – Open**		
Date of review of security classification			
Authority	FFA Director of Fisheries Operations		
Author	MCS Specialist		
Documentation status	☑ Working draft	Consultation release	Final version

1. Purpose

ISMS Policy Statement – FFA MCS Regional Information Management Facility (RIMF) defines FFA policy with regard to the security of information within and distributed from the FFA RIMF.

The RIMF's overall objective is to facilitated easy, integrated access to diverse data to support member's decision making on a wide range of fisheries MCS, management, development and administration issues.

RIMF provides FFA members the following services:

- a data warehouse and custodianship for the collection, storage, quality assurance and dissemination of data;

- analysis and value-adding of MCS data and information to support MCS activities; and

- desensitising information to facilitate sharing of MCS data.

2. Scope

The scope of *ISMS Policy Statement 1B – RIMF* is information and information systems that make up, or is a part of, the RIMF. It applies to all RIMF users and RIMF administrators.

The policy conjuncts and support *ISMS Policy Statement 1A – Data Access & Use,* providing additional and specific controls for RIMF data and information security.

3. Risks

RIMF provides custodianship and is a distribution hub of sensitive commercial and national security information for 17 FFA member countries. Certain elements of the RIMF are available to Recognised Quadrilateral Surveillance Providers (AU, NZ, FR, and US) under the terms of ISMS Policy Statement 8. The high number of users and their diversity is a risk to be managed through uniform and universally agreed security standards.

For the purposes of this policy and the maintenance and adherence to data access rules under the ISMS, the Niue Treaty Subsidiary Agreement is considered to be part of the RIMF.

Information security risks regarding this RIMF information arise through (1) oversight of subsequent variations to authorisations, (2) interpretation of what has been agreed to be shared, and (3) changes in product for distribution which is not captured under existing data sharing agreements.

The risk of inadvertent release, access or distribution of RIMF data contrary to agreement of the Data Owner (in most cases FFA members) is ameliorated through FFA policy which sets out the terms, conditions, and reason for physical or electronic access to the RIMF.

4. Policy

RIMF authorised personnel and access groups will be maintained in the online register established in section 5.3 of the ISMS. The Secretariat will maintain the ability to issue user specific authorisations that only allow the user to access certain elements of the RIMF in accordance with the permissions granted by Data Owners and the authorisation requested by Official Contacts.

The conditions and undertakings of FFA employees and contractors to access RIMF data are described in Annex A of ISMS Policy Statement 3.

Prior to RIMF access all other users and administrators will agree to the terms in Annex B of ISMS Policy Statement 1A.

Access and use to RIMF classified information will be in accordance with *Table 1: RIMF Data Access & Controls*.

Rooms, buildings and installations accredited to be part of the RIMF are:

- The Regional Fisheries Surveillance Centre – being the secured room attached to the FFA Conference Centre; and
- The “Bunker” being the secured stand-alone building at the western end of the main FFA office building.

The Director-General will accredit, by amendment to this Policy Statement, an area, room, group of rooms, buildings, or installation to be a part of the RIMF when satisfied that the space has extraordinary security safeguards to prevent and detect visual, acoustical, technical, and physical access by unauthorized persons. Refer to *Annex A: Accredited RIMF Areas*.

5. Compliance

Refer to section 5 of Policy Statement 1A.

Annex A: Accredited RIMF Areas

The security measures for an accredited RIMF Area include:

Personnel Controls

- Access rosters listing persons authorised access to the facility are maintained at the RIMF point of entry, using a combination of electronic coded security identification cards and security access rosters.
- Visitor identification and control using a security access register is used to identify and control visitors seeking access to the RIMF Area.
- Non-MCS authorised personnel entering the RIMF Area must be continuously escorted by personnel authorised to be within the RIMF Area.

Building Construction

- The perimeter walls, floors and ceiling are permanently constructed and attached to each other. Construction has been done in a manner to provide visual evidence of unauthorized penetration.
- The RIMF Area perimeter walls, doors, windows, floors and ceiling, including all openings, provide sufficient sound attenuation to preclude inadvertent disclosure of conversation.
- The RIMF Area houses an internal operational vault for highly sensitive information. The vault has no windows, no doors, is permanently constructed, and equipped with an automatic door closer and an access control device.
- Primary RIMF Area entrance is limited to one door. A secondary door exists but is only used as an emergency exit.
- All RIMF Area doors are closed when not in use, with the exception of emergency circumstances. The doors if left open for any length of time due to an emergency or other reasons, will be controlled in order to prevent unauthorized removal of information.
- The RIMF Area perimeter doors are plumbed in their frames and the frame firmly affixed to the surrounding wall. Door frames are of sufficient strength to preclude distortion that could cause improper alignment of door alarm sensors, improper door closure or degradation of audio security.
- The RIMF Area primary entrance door is equipped with an automatic door closer and an access control device.
- The RIMF Area is located in a controlled area secured by two permitter fences, each with controlled access points. The outer permitter has a 24-hour manned security presence. The inner perimeter is reinforced steel, controlled locking device, fenced with reinforced material from ground to height of building.
- The RIMF Area emergency exit door is constructed of material equivalent in strength and density to the main entrance door. The door is secured with deadlocking panic hardware on the inside and has no exterior hardware.
- The RIMF Area will be fitted with a local enunciator in order to alert people working in the area that someone entering the facility entered or exited the RIMF Area due to an emergency condition or is an unauthorised MCS person.
- RIMF Area door construction is a solid wood core door, 144 millimetres thick.
- All vents, ducts, and similar openings that enter or pass through the RIMF Area are protected with either bars, or grills, or metal duct sound baffles.

- All windows are equipped with drapes and metal gauge to preclude visual surveillance of personnel, documents, material or activities.
- All windows are covered with materials which provide protection from forced entry. The windows are inoperable from the outside.

ISMS Policy Statement 3: Human Resource Security

Document Details
Author: Fisheries Operations Division
Version: 1.0
Document Status: Approved FFC110

Security classification	**Unclassified - Open**		
Date of review of security classification			
Authority	FFA Director of Fisheries Operations		
Author			
Documentation status	☑ Working draft	Consultation release	Final version

1. Purpose

ISMS Policy Statement 3 – Human Resource Security provides additional information security control with respect to implementation and maintenance of the FFA ISMS by individuals.

The policy sets out how all FFA personnel and contractors assigned responsibilities as defined in the FFA ISMS are competent to perform the required tasks, are aware of the relevance and importance of their information security activities, and understand how they contribute to the achievement of the ISMS objectives.

2. Scope

This policy applies to all FFA staff and contractors.

FFA's human resources are the most important component in maintaining the safety and security of FFA information and information systems. Each individual contributes to the safe and secure use of information and information systems that FFA holds on behalf of its member countries.

3. Risks

The FFA Secretariat holds sensitive information which may be put at risk if users do not follow the ISMS. Every user of FFA information and information systems is a risk and a possible threat to FFA information security. They also represent a vulnerability that might be exploited by external threats.

4. Policy

Verification checks will be carried out on all new employees and contractors.

During employment and as part of FFA's ISMS implementation, FFA will ensure that all employees, contractors and third party users are familiar with the ISMS, aware of information security threats and concerns, their responsibilities and liabilities, are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error. All employees of the organisation and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function. In order to achieve this, FFA will, as a priority, develop specific interactive training materials for staff (audio-visual and presentational material) that all existing staff will need to review and that will be extended to new staff on arrival. Simple fact sheets on key aspects of the ISMS, such as examples of the classification of different data types and checklists for how to treat that data.

At termination of employment, contract or agreement, FFA shall ensure all employees, contractors and third party users return all FFA assets in their possession. The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

All FFA employees, contractors and agents will be required to enter an *FFA ISMS Agreement* (Annex A) prior to accessing FFA's information and information systems.

5. Compliance

Refer to section 5 of Policy Statement 1A.

Annex A: Information Security Agreement for Employees & Contractors

I will make myself familiar with FFA’s Information Security Management System (ISMS) and its policies, procedures and any special instructions that relate to information security.

I will not transmit information that I know, suspect or have been advised is of a higher level of sensitivity than the system is designed to carry.

I will not transmit information that I know or suspect to be unacceptable within the context and purpose for which it is being communicated.

I will not make false claims or denials relating to my use of FFA information and information systems.

I will protect any classified material electronically sent, received, stored or processed by me to the same level as I would paper copies of similar material and to the level required in the ISMS.

I will appropriately label information using FFA’s information classification scheme.

I will not send sensitive or confidential information over public networks such as the internet unless it is suitably protected via encryption or other means.

I will always check that the recipients of e-mail messages are correct so that potentially sensitive or confidential information is not accidentally released into the public domain.

I will not auto-forward email from my FFA e-mail account to an email account outside of FFA.

I will not forward or disclose any sensitive or confidential material received except in accordance with the rules of the ISMS and unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel.

I will seek to prevent inadvertent disclosure of sensitive or confidential information by taking care when printing information received electronically and by carefully checking the distribution list for any material to be transmitted.

I will securely store or destroy any printed material.

Classified material shall not be left unattended at my work station and at the end of each working day, my work station shall be free from all removable documents including post-it notes, business cards, and removable media (e.g. CDs, DVDs, memory sticks etc) that contain any classified information.

I will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received (this might be by logging-off from the computer, activating the password-protected screensaver, etc., so as to require a user log-on for activation).

Where FFA IT has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked requiring a user log-on for reactivation), then I will not attempt to disable such protection.

I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security.

I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended.

I will not remove equipment or information from FFA's offices without permission.

I will take precautions to protect all computer media and portable computers when taking them outside of FFA's offices.

I will not deliberately introduce viruses, 'Trojan horses' or other malware into FFA's computer systems.

I will not disable anti-virus protection installed on my computer.

I will comply with legal, statutory or contractual obligations which the FFA informs me are relevant.

I will manage my e-mail and extranet accounts in accordance with FFA ISMS.

Name: ____

_

Position: ____

_

FFA Division/Title of Consultancy Contract: ____

Signature: ______________________________ Date: ______________________

ISMS Policy Statement 4: Appropriate Use of E-mail, Social Media and Other forms of Electronic Communication

Document Details

Author: Fisheries Operations Division
Version: 1.0
Document Status: Approved FFC110

Security classification	**Unclassified – Open**		
Date of review of security classification			
Authority	FFA Director of Fisheries Operations		
Author			
Documentation status	☑ Working draft	Consultation release	Final version

1. Purpose

ISMS Policy Statement 4 – Appropriate Use of E-mail, Social Media and Other forms of Electronic Communication defines FFA policy concerned with the use of FFA e-mail accounts, and the communication of information using social media or other electronic communication such as Skype or Facebook Messenger. This policy exists ensure effective and appropriate use of FFA systems and hardware in a manner which maintains the security of its information.

The term “e-mail” below is used to cover all forms of electronic communication.

2. Scope

This policy applies to all staff and employees of FFA and any other person granted access to FFA’s computer network.

All users of FFA’s IT facilities must understand and use this policy. Users are responsible for ensuring the safety and security of FFA’s systems and the information that they use or manipulate.

All users have a role to play and a contribution to make to the safe and secure use of e-mail.

3. Risks

E-mail and other communication tools are provided to staff to assist them in carrying out their duties communicating efficiently and effectively with other staff members, other companies and partner organisations.

E-mails may contain inappropriate content that should not be viewed by users.

E-mails may contain malicious code which has the potential to access or damage data or forward data to a third party.

4. Policy

Use of Email

FFA's e-mail facilities are primarily for business use. Occasional and reasonable personal use of e-mail is permitted on staff members' own time subject to the conditions set out in the FFA ISMS.

When using FFA's e-mail facilities for business purposes, Users will comply with the rules set out in FFA's Information and Communication Technology Manual (link).

Accidental viewing of materials which infringes this policy should be reported according to the Information Security Incident Reporting Procedure.

Monitoring of E-mail Use

All e-mail coming into or leaving FFA is scanned for viruses and offensive material.

The use of e-mail is recorded and may be monitored. It is possible to identify the senders, recipients and content of e-mail.

FFA reserves the right to inspect any files at any time during investigations where there is suspected misuse and to withdraw access to e-mail.

Personal Use of Email

Personal use is defined as any activity that is not work-related or necessary in the performance of duties connected to employment with FFA.

Staff may use on an occasional basis FFA computers for personal use to send and receive e-mail. The personal use of e-mail for any purpose must not be excessive. It does not count as working time and must not interfere or detract from FFA's business or work. It should also not distract any other staff member from their work.

Staff using FFA computers waive any rights to privacy regarding personal information on FFA's computers and accept, as a condition of doing so, that their activity may be monitored.

No liability can be accepted by FFA for any loss that an individual may suffer as a result of personal use of FFA's computers.

Support must not be requested from other employees for personal use of e-mail.

Subscription to e-mail mailing lists or list servers for personal purposes is not allowed.

Using e-mail for personal purposes must comply with the principles set out in FFA's ISMS.

Phishing

FFA IT will ensure that specific awareness material about phishing is included in education to be developed and promulgated under ISMS Policy Statement 3. Users must not run software or click on a link to verify their password; this is to avoid deceit by ‘phishing’.

Purchasing of Goods or Services

The purchasing of goods or services via e-mail is subject to FFA’s Financial Regulations and Finance Manual (links). These must be consulted to determine which goods and services are permissible to purchase.

Computer viruses and malicious programs

Computers can be infected by viruses and malicious programs by opening an attachment to an e-mail or just visiting a link to a webpage contained within the e-mail.

If any FFA staff believes they have a computer virus, it should be reported to the IT Service Desk immediately.

Masquerading

It is an offence to masquerade as another person via e-mail and to send e-mails in another person’s name.

It is an offence to manipulate e-mails so as to alter content or suggest that they have been sent at a different time to when they were originally sent or from a different location or computer.

Legal Compliance

Electronic communications and files are admissible in court as evidence. Staff must not not write anything about anybody that cannot proved and evidenced.

5. Compliance

Refer to section 5 of Policy Statement 1A.

ISMS Policy Statement 5: Information Backup

Document Details
Author: Fisheries Operations Division
Version: 1.0
Document Status: Approved FFC110

Security classification	**Unclassified - Open**		
Date of review of security classification			
Authority	FFA Director of Fisheries Operations		
Author			
Documentation status	☑ Working draft	Consultation release	Final version

1. Purpose

ISMS Policy Statement – Information Backup defines FFA's overall policy for backing up the organisation's information and software application systems. The aim is to ensure that it is always possible to recover information and application systems.

2. Scope

This policy applies to:

- all electronic information stored upon FFA's servers and PCs / laptops.

- all FFA application systems, application software and their configuration.

3. Risks

Information can be lost as a result of crashed disks, deletion, or corruption, therefore integrity and availability of important information needs to be maintained by making regular copies to other media.

4. Policy

Specific details of backup strategies and procedures are spelled out in the FFA Information and Communication Technology Manual (link). Overarching policy guidance includes:

- Servers and systems will be backed up using combination of suitable backup methods including internet backup, and mirrored servers at a remote site.

- Backups will be performed using dedicated backup software appropriate for the operating system being used.

Information backup is also a key component of FFA's Business Continuity Plan (link).

5. Compliance

Refer to section 5 of Policy Statement 1A.

ISMS Policy Statement 6: INFRASTRUCTURE HARDENING

Document Details
Author: Fisheries Operations Division
Version: 1.0
Document Status: Approved FFC110

Security classification	**Unclassified - Open**		
Date of review of security classification			
Authority	FFA Director of Fisheries Operations		
Author			
Documentation status	☑ Working draft	Consultation release	Final version

1. Purpose

ISMS Policy Statement – Infrastructure Hardening defines FFA's policy to be followed for infrastructure hardening.

Hardening is the process of securing a system by reducing its surface of vulnerability. By the nature of operation, the more functions a system performs, the larger the vulnerability surface.

Most systems perform a limited number of functions. It is possible to reduce the number of possible vectors of attack by the removal of any software, user accounts or services that are not related and required by the planned system functions. System hardening is a vendor specific process; as different system vendors install different elements in the default install process.

The possibility of a successful attack can be further reduced by making it difficult for a potential attacker to identify the system being attacked so that the attack cannot easily exploit known weaknesses.

2. Scope

This policy applies to all components of the information technology infrastructure and includes:

- Computers;
- Servers;
- Application Software;
- Peripherals;
- Routers and switches;
- Databases; and
- Telephone Systems.

All FFA IT staff must understand and use this policy. FFA IT staff is responsible for ensuring that the IT infrastructure is hardened and that any subsequent changes to systems do not affect the hardening of the systems.

3. Risks

Hardening is required to increase FFA’s resilience to the following risks:

- Attack by external systems or users seeking to damage infrastructure, compromise, destroy or access data or commit other damage and fraud;
- Inefficiency through lack of a Standard Operating Environment and the economies of scale that a SOE allows;
- Loss, damage or decreased operation as a result of non-standard software and hardware not interacting with the SOE correctly or efficiently.

4. Policy

Specific details of backup strategies and procedures are spelled out in the FFA Information and Communication Technology Manual (link). Overarching policy guidance includes:

All new systems will undergo a specified hardening process.

Only software that has been approved for use by the IT department may be installed on FFA’s computing devices.

Non-essential software applications and services will be uninstalled or disabled as appropriate.

Servers, PC’s and laptops will be configured to prevent the execution of unauthorized software.

All PC’s and laptops will be built from a standard image. Any change to the standard image must be supported by a business case.

Access to the local administrator account will be restricted to members of FFA IT to prevent the installation of unauthorized software and the modification of security software and controls.

5. Compliance

Refer to section 5 of Policy Statement 1A.

ISMS Policy Statement 7: Appropriate use of Internet

Document Details

Author:	Fisheries Operations Division
Version:	1.0
Document Status:	Approved FFC110

Security classification	**Unclassified - Open**		
Date of review of security classification			
Authority	FFA Director of Fisheries Operations		
Author			
Documentation status	☑ Working draft	Consultation release	Final version

1. Purpose

ISMS Policy Statement – Appropriate Use of Internet defines FFA policy to ensure effective use of time, prevent illegal and inappropriate use of the internet and minimise security exposure of FFA's information and information systems to the internet.

2. Scope

This policy applies to all FFA staff, contractors and any other user given access to FFA's computer network or hardware.

All users of FFA's IT facilities must understand and use this policy. Users are responsible for ensuring the safety and security of FFA's systems and the information that they use or manipulate.

All users have a role to play and a contribution to make to the safe and secure use of the Internet.

3. Risks

Internet access is provided to staff to assist them in carrying out their duties efficiently and effectively. This facilitates access to a vast range of information available on the world-wide web and the communication with people outside of FFA.

A large number of sites exist on the internet that contains inappropriate content and it is important that this content is not downloaded to FFA's computer systems. Many other sites contain malicious software which could harm FFA's computer systems if deliberately or inadvertently downloaded.

4. Policy

FFA's internet access is primarily for business use.

When using FFA's internet access facilities, Users will comply with the rules and guidelines set out in FFA's Information and Communication Technology Manual (link).

A corporate internet filter is utilised to prevent specific types of websites being accessed.

Websites which need to be accessed to conduct FFA's business but are blocked can be made available by contacting FFA IT Helpdesk. Authorisation will be required before access is granted.

Accidental viewing of materials which infringes this policy should be reported according to the Information security incident reporting procedure.

Personal use of the Internet

Personal use is defined as any activity that is not work-related or necessary in the performance of duties connected to your employment.

Staff may use on an occasional basis FFA's computers for personal use to access the Internet as long as it complies with the principles set out in this FFA ISMS.

Staff who use FFA's computers for personal use to access the Internet must accept, as a condition of doing so, that their activity may be monitored and waive any rights to privacy regarding personal information on FFA's computers.

The personal use of the Internet for any purpose must be in the employee's own time and must not interfere with employee productivity.

Users should seek to keep any costs incurred as a result of personal use of the Internet to a minimum.

No liability can be accepted by FFA for any loss that an individual may suffer as a result of personal use of FFA's computers.

Support must not be requested from other employees for personal use of the internet.

The playing of internet computer games is not allowed.

Using the Internet for personal purposes must

Purchasing of goods and services

The purchasing of goods or services via the Internet is subject to FFA's Financial Regulations and Finance Manual (links).

Masquerading

It is an offence to masquerade as another person on the internet and post articles in another person's name.

Legal compliance

The Internet must be used for lawful purposes only, and must comply with relevant legislation.

Users will be placed at at risk of prosecution if unlawful action is involved.

Electronic communications and files are admissible in court as evidence. Do not write anything about anybody that you cannot prove and evidence.

5. Compliance

Refer to section 5 of ISMS Policy Statement 1A.

ISMS Policy Statement 8: Arrangements for sharing of data and information between FFA Members, FFA Secretariat and Recognised Quadrilateral Surveillance Providers

Document Details

Security classification	**Open**
Date of review of security classification	July 2017
Authority	Director-General
Author	Deputy Director-General
Documentation status	Final Version (v6.0)

1. Purpose

1. This ISMS Policy Statement defines FFA policy concerning:

   a. the sharing and use of information held on behalf of the FFA members with Recognised Quadrilateral Surveillance Providers (RQSP) as defined below;

   b. the sharing of information held on behalf of the FFA members with regional Rescue Coordination Centres (RCCs) for the purposes of Safety of Life at Sea (SOLAS) and Search and Rescue (SAR); and

   c. the sharing of data and other information generated by RQSP with the FFA Secretariat.

2. This ISMS Policy Statement is to be read and applied in conjunction with the ISMS generally and ISMS Policy Statement 1A specifically. Where there is an explicit inconsistency between this ISMS Policy Statement and ISMS Policy Statement 1A, the provisions of this ISMS Policy Statement will apply.

2. Scope

3. The scope of this ISMS Policy Statement is information held within FFA Data Resources, with a particular focus on Monitoring, Control and Surveillance (MCS) related data, especially the Regional Surveillance Picture (RSP) and Vessel Monitoring System (VMS) information.

4. Information collected by air assets operating under FFA command and control as part of the Australian funded Pacific Security Maritime Program (PMSP) is also relevant to this ISMS Policy Statement. It is the FFA's intention that this information will be integrated into the RSP, and primarily available to RQSP through that means.

5. This ISMS Policy Statement applies to all employees of FFA and to the handling of information exchanged with RQSP agencies as described and defined below.

2.1 Recognised Quadrilateral Surveillance Providers

6. RQSP is a generic term intended to cover agencies of the Quadrilateral Defence Coordination Group (Australia, France, New Zealand and the United States of America)

that are directly involved in supporting the fisheries MCS efforts of FFA members through the provision of air or surface surveillance assets. RQSP includes the designated Rescue Coordination Centres for the Quadrilateral Defence Coordination Group.

7. The following agencies are considered as RQSP, noting that this list may be updated from time to time. Note the following list identifies the operational centres where data will be received for the purpose of informing asset deployment.

   a. Australia:

      i. Maritime Border Command

      ii. Joint Operations Command

   b. France:

      i. Forces armées de la Nouvelle-Calédonie (French Armed Forces of New Caledonia) including Joint Headquarters, French Navy, French Air Force and Maritime Rescue Coordination Centre

      ii. Forces armées de Polynésie Française (French Armed Forces of French Polynesia) including Joint Headquarters, French Navy and French Air Force + Maritime Inter Agency Centre / Maritime Information Fusion Centre (MIAC / IFC)

   c. New Zealand:

      i. National Maritime Coordination Centre

      ii. Headquarters Joint Forces New Zealand

      iii. Rescue Coordination Centre New Zealand

   d. United States of America

      i. United States Coast Guard

      ii. United States Navy

8. RQSP agencies and personnel that receive data and information under this ISMS Policy Statement are understood to be “data users” as defined in ISMS Policy Statement 1A.

3. Risks

9. This ISMS Policy Statement addresses the following risks:

   a. Use or sharing of FFA member MCS data for purposes outside of direct support to FFA fisheries MCS efforts and SAR efforts, noting that this information is classified in the two highest tiers (Classified High – RED and Classified Medium – YELLOW) under the ISMS Policy Statement 1A; and

   b. Ineffective or inefficient deployment of RQSP assets due to incomplete maritime domain or situational awareness.

4. FFA Policy

10. The policy statements below describe both the data and information that FFA will provide to RQSP in their direct support to FFA fisheries MCS efforts, and the RQSP roles as regional Rescue Coordination Centres, and the data and information that is expected to be provided by RQSP to FFA in respect of that direct support.

4.1 Reasons for sharing data with RQSP

11. FFA and FFA members recognise the generous support offered to them by RQSPs through the provision of assets and associated technical capacity. Despite enormous growth in national capacity through a number of means, notably enhanced data sharing, formalised compliance officer training, and the PMSP replacement of Pacific Patrol Boats (PPBs) and incoming aerial surveillance capability, FFA members will continue to rely on RQSP for assistance in their fisheries MCS efforts.

12. While there are undoubtedly additional benefits to both FFA members and RQSP, the primary purpose of sharing data with RQSP is to secure efficient and effective support to regional and national MCS efforts.

13. Data is primarily provided to RQSP to ensure adequate planning and profiling to inform efficient and effective asset deployment in support of planned regional operations, bilateral and sub-regional operations and opportunistic patrols conducted from time to time or following the spontaneous request for support of any FFA member.

14. Data is also provided to RQSP to assist them to fulfil their roles as regional Rescue Coordination Centres.

4.2 Data and information provided to RQSP

15. FFA will provide each RQSP with data and information as follows:

Data Type	Modality of Provision
Regional Surveillance Picture	Near real time Data transmitted to RQSP in OTH-G format via e-mail FFA will be seeking more secure formatting such as encrypted e-mail or Internet Transfer Protocol in the future
Vessel Monitoring System positional data	Near real time Data made available through a single log-in for each RQSP to the FFA VMS (TrackWell) system.

4.3 Storage, use, protection, destruction and sharing of data provided to RQSP

16. Data provided to RQSP as described above will be treated in accordance with the following provisions, which apply to all forms of FFA provided data:

    a. All usage of data and information will be compatible with the reasons for data sharing outlined in section 4.1.

b. All data and information is to be stored in a manner that is consistent with the ISMS and affords it the protection of other similarly sensitive data that the RQSP agency handles.

c. Data and information are only to be accessible to RQSP agency personnel that hold security clearances as determined necessary by that agency for access to other forms of similarly sensitive data.

d. Any FFA member that provides data to FFA is considered to be the owner of that data. No data may be further used or shared other than as contemplated in this ISMS Policy Statement without the express consent of the data owner.

e. Outside of the RQSP agency, data (either in its provided or processed form) is only to be provided directly to assets actively deployed in support of FFA Member fisheries MCS efforts or conducting SAR under the direction of a regional Rescue Coordination Centre. It is not to be shared with any entity, agency or organisation other than RQSP listed above.

f. Until such time as broader law enforcement mandates for cooperation under the FFA framework are agreed upon, any issues or incidents that are based on FFA provided data, but not fisheries MCS related should only be actioned with the authorisation of the FFA member(s) who owns the data, as determined by FFA policy. This provision is not intended to limit law enforcement action otherwise permissible under international law.

g. Any RQSP wishing to publish or publicise products or analysis derived through its analysis should consult with the affected individual members through the FFA Director-General. To illustrate presentations of RQSP, FFA will provide appropriately sanitised data to be used in official documents or slide shows that may be potentially shared with non-RQSP agencies.

h. The data files described above that are forwarded from FFA to each RQSP, including any authorised copies made, are to be destroyed as soon as practical, or within three months after receipt unless it is part of an investigation or review or required to be retained in accordance with an RQSP's domestic legislation;

i. It is acknowledged that removal or destruction of information that has been integrated into Common Operating Pictures with other RQSP data may not be possible. In such cases, RQSP will store and archive any retained information in a manner that restricts access and sharing in accordance with paragraphs 16 (a) to (g) above.

j. RQSP personnel will promptly notify the FFA Director-General, in writing, of any unauthorised, negligent or inadvertent disclosure of data provided to them by FFA.

4.4 Data and information to be provided to FFA

17. Reciprocity is a key element to any sharing arrangement and the value of the relationship between RQSP, FFA members and FFA would be substantially enhanced through increased two-way communication. The following guidelines are set forth to encourage mutual cooperation.

Scenario	**Data Type**	**Modality for provision**
1. Supporting any of the 4 “named” FFA Regional Operations[3]	Prior notification of assets to be provided and broad areas of operation Indication whether an FFA member air/sea rider may be embarked on board for the mission.	In accordance with the operational directives issued by FFA prior to each operation
	Deployment characteristic and finer scale definition of area of operation (recognising and respecting the need for operational security, particularly of military assets)	14 days prior to commencement of operation
	Actual patrol plans	Daily during operations
	• Sighting information • Boarding and inspection information including actual or potential breaches detected • Photographic or other evidence collected • Post mission reports	Daily during operations, with preference for real-time or worst case of 5 hours after patrol completion
2. Deploying assets for MCS support to FFA members as a primary or secondary mission objective outside of named operations	Deployment characteristic and definition of area of operation (recognising and respecting the need for operational security, particularly of military assets)	14 days prior to commencement of operation Potential for diplomatic notes to be copied to FFA
	Actual patrol plans	Daily during operations
	• Sighting information • Boarding and inspection information including actual or potential breaches detected • Photographic or other evidence collected • Post mission reports including operationally relevant metrics	Daily during operations, with preference for real-time or worst case of 5 hours after patrol completion

18. The primary use of this information will be to integrate it into the RSP. Any use, dissemination or analysis of this information will be in accordance with the ISMS, and particularly ISMS Policy Statement 1A.

[3] Operations Rai Balang, Island Chief, Tui Moana, Kuru Kuru

5. Disputes

19. Any disputes arising from the sharing or use of information under this ISMS policy Statement will be notified to other relevant participants as soon as possible.

20. Disputes will be resolved, as far as possible, through consultation between the individual participants (FFA member(s), FFA Secretariat and RQSP(s)) that are impacted upon by the disputed issue. Where there is a dispute relevant to a specific FFA member or members, the FFA Secretariat may play a facilitation role.

21. All participants will approach any such consultation on the basis of the mutual benefits that sharing or use of FFA member MCS data provides.

22. In the event that such consultations are unable to produce a mutually acceptable agreement or solution within 3 months of the matter will be referred to FFC (on the part of FFA Secretariat) and capitals (on the part of RQSP and FFA members) for consideration and resolution.

23. Solutions to any incident arising will pay particular attention to ISMS Policy Statement 1A, which provides data owners (individual FFA members) with the ultimate discretion over their individual data.

6. Compliance

24. If any FFA employee is found to have breached this ISMS Policy Statement, they may be subject to disciplinary action as per the FFA Staff Regulations.

25. Any violation of this ISMS Policy Statement by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.

26. Any violation of this ISMS Policy Statement by a Data User may result in suspension of data access privileges to a period of time as determined by the FFC.

27. It is acknowledged that no RQSP is bound by the guidelines set out in this policy statement. However, FFA and FFA members consider mutual cooperation and reciprocity in information sharing to be of high importance and the level of adherence to the guidelines and associated increases in the level and timeliness of information provided to FFA will be used in ongoing assessments of this ISMS Policy Statement in the future.

ANNEX A: RECOGNISED QUADRILATERAL SURVEILLANCE PROVIDER CONFIDENTALITY AND RECIPROCITY ARRANGEMENT UNDER FFA ISMS POLICY STATEMENT 8: ARRANGEMENTS FOR SHARING OF DATA AND INFORMATION BETWEEN FFA MEMBERS, FFA SECRETARIAT AND RECOGNISED QUADRILATERAL SURVEILLANCE PROVIDERS.

Data User(s)

Recognised Quadrilateral Surveillance Provider(s) (see section 2.1 of ISMS Policy Statement 8)

Purpose and details of the data to be used

Monitoring, Control and Surveillance data as described in section 4.2 of FFA ISMS Policy Statement 8.

Operational Point of Contact(s)

Full name	Role Or Title	Contact Details

Declaration

The RQSP intend to act in accordance with FFA policies to the fullest extent possible in accordance with their respective domestic laws, regulations, and policies. The signing of this confidentiality and reciprocity arrangement reflects a political commitment. It does not constitute a legally binding commitment, and does not impose, nor is it intended to impose, any legal commitments.

On behalf of the Recognised Quadrilateral Surveillance Provider(s), the Primary Authorisation and Accountability Representative:

- Acknowledges that any information provided by FFA will be used for a purpose described in section 4.1 of FFA ISMS Policy Statement 8, subject to the respective domestic laws, regulations, and policies of the RQSP;

- Acknowledges that any information provided by FFA will be used and managed in accordance with the provisions in section 4.3 of FFA ISMS Policy Statement 8, subject to the respective domestic laws, regulations, and policies of the RQSP;

- Will use best efforts to provide open communications and notifications to FFA as set out in the guidelines in section 4.4 of ISMS Policy Statement 8, subject to the respective domestic laws, regulations, and policies of the RQSP. When requested by the FFA the RQSP will, when permitted to do so under its domestic laws, regulations and policies, provide an explanation of such domestic laws, regulations or policies in the event that they prevent communication of information set out in section 4.4;

- Notes the potential results of actions inconsistent with aspects of ISMS Policy Statement 8 as described in section 6 therein; and

- Will provide notification to the Director-General of FFA within 15 days of any change in the Operational Point of Contact.

Duration

The operation of this arrangement will be reviewed by the MCS Working Group from time to time.

Signed on behalf of the Recognised Quadrilateral Surveillance Provider(s) by the Principal representing <country> in the Defence Quadrilateral Coordinating Group:

Full name	Role or Title	Contact Details	Signature and Date

[i] The FFA ISMS Committee is separate from the FFA Security Committee which meets on an ad-hoc basis and has a mandate to advise on general security issues in Honiara.