Pacific Islands Forum Fisheries Agency (FFA)

Information Security Management System

Document Details

Author:	Fisheries Operations Division
Version:	1.0
Document Status:	Pending:

1. FFA internal consultation
2. MCS Working Group consultation and recommendation to FFC
3. FFC approval

Security classification	**Open**		
Date of review of security classification			
Authority	Director General		
Author			
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:

- To protect the organisation's information 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.
- To meet its custodianship responsibilities with respect to warehousing, storing, quality assurance and dissemination of data held on behalf of FFA members.

The Information Security Management System (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.

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. It is envisaged that Data Users of members who access and use *shared* data held within FFA information systems are likewise bound by a nationally-developed Information Security framework similar in scope to the FFA ISMS.

The Information Security Policy applies to all forms of information including:

- Speech, spoken face to face, or communicated by phone or radio;
- Hard copy data printed or written on paper;
- Information stored in manual filing systems;
- Communications sent by post / courier, fax, electronic mail;
- Stored and processed via servers, PC's, laptops, mobile phones, PDA's; and
- 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 2700 the International Standards for Information Security and is structured to include the main security category areas within these standards.

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. 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 organization.

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, will be incorporated into the ISMS.

FFA will work towards implementing and maintaining the ISO2700 standards, the International Standards for Information Security.

All breaches of information security, actual or suspected, must be reported and will be investigated with the results of the investigation and any subsequent action being reported to FFC.

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

FFA's Security Committee [Division Directors] will 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.

The Security Committee [Division Directors] will assess if the ISMS Statements 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 implementing polices to assist Authorised Users and System Custodians to meet their Information Security responsibilities.

The Director-General approves all editorial changes and changes to the ISMS as identified by the Security Committee [Division Directors] or System Custodian. Substantive policy changes will be made in consultation with all Division Directors subject to approval of the Director-General and endorsement by the Forum Fisheries Commission (FFC).

5.3. Information Security Responsibilities

Individuals

All staff and employees of the organisation, contractual third parties, and agents of the organisation accessing FFA information are required to adhere to the Information Security Policy, processes and procedures.

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 IT Helpdesk.
- 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 him by reason of his official position without obtaining prior permission of the Director-General, FFA at all times during and after termination of employment.

Failure to comply with the FFA ISMS and its processes and procedures will lead to disciplinary and remedial action.

If any FFA employee is found to have breached this Information Security Policy they may be subject to disciplinary action.

Any violation of the policy by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.

Division Directors

Division Directors 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;
- Information risk assessments and business continuity planning are undertaken;
- Security measures are tested, reviewed and revised regularly;
- That appropriate data access privileges are provided for staff members within their Division; and
- All major systems and information assets are accounted for and have a nominated “System Custodian” who is responsible for the implementation and management of the ISMS in relation to those assets.
- Isolating or disconnecting immediate and serious threats to Information Systems and assets.

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 and recommending access requests, data classification and sharing requirements, to the appropriate Division Director;
- Reviewing access rights and privileges of existing approved users for validity and providing access recommendations to the appropriate Division Director;
- 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 will be designated by Divisional Directors, unless specified below:

System or information asset	**Security Custodian:**
FFA Secretariat system platforms (eg. 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:	SOO
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.

Owners will be identified for all assets and they will be responsible for the maintenance and protection of their assets.

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.

Verification checks will be carried out on all new employees and contractors. Where possible, verification checks will be made on all third parties.

8. Physical and Environmental Security

Classified (non-public domain) information processing facilities will be housed in secure areas.

Secure areas are and will be protected by defined security perimeters with appropriate security barriers and entry controls.

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

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. ISMS Statements are Annexed and form a component of the ISMS.

Segregation of duties will be implemented where appropriate to reduce the risk of negligent or deliberate system misuse.

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 the Director General.

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.

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 IT Manager, the Director of Fisheries Operations and, if applicable, relevant Division Director(s) will assess the incident or vulnerability controls in place and make an escalation determination for notifying the Deputy Director General and Director General. Escalation to this level will generally occur where the incident posses an unacceptable information security risk to FFA.

The Security Committee will consider all reported security incidents oversighting recourse and remedial action reporting to the Director General of all incidents until the security risk of each incident is acceptably managed.

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.

Divisional Directors are responsible for undertaking business continuity management processes to minimise the impact on the organisation and recover from loss of information assets. This includes undertaking risk assessments to assess the business impact of disasters, security failures and loss of service or service availability.

14. Compliance

FFA will ensure the ISMS upholds any statutory and regulatory law or contractual obligations affecting its information systems.

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 organization
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.

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
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 1A: Data Access and Use

Document Details

Author: Fisheries Operations Division
Version: 1.0
Document Status: Pending:

- MCS Working Group consultation and recommendation to FFC
- FFC approval

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.

Note: *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.

2. Scope

The scope of the *ISMS Policy Statement – Data Access and Use* is information held within FFA Data Resources. It applies to all employees of FFA 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 holds 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 Country level; that is, a specific set of data is deemed to be owned by a particular Country.

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 owner, data will be accessed according to the rules applicable to the confidentiality classification of such data.

- 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.

- Data Users cannot disseminate information they are authorised to access to another party unless such party is also an authorised user of the same data.

- 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 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.

- Individuals will observe a ‘clear desk policy’ for unattended classified information. Unattended computers must be in such a state as to minimize the risk of unauthorised disclosure of information sent or received. These actions may include logging-off from the computer or activating the password-protected screensaver so as to require a user logon for activation.

- 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 :

5. Compliance

If any FFA employee is found to have breached this Information Security Policy they may be subject to Disciplinary action.

Any violation of the policy by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.

Any violation of the policy by a Data User may result in suspension of data access privileges to a period of time as determined by the FFC.

Table 1: Information Security Classification Guidelines

When should it be used?	Classification	How Should it be shared?	E.g. Information / Data Types
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. (Annex A & B provide template authorisation and acceptance forms) Internet exchanges will use at a minimum Hypertext Transfer Protocol Secure (HTTPS), with individual user accounts for web based portals or email exchange	Commercially sensitive material including fine scale catch and effort data, access agreements. MCS compliance analysis and profiling for deriving risk levels of: ○ Persons of interest ○ Vessels compliance risk
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) FFA VMS FFA RFV – all details
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.	FFC and subcommittee papers and briefings e.g. Management Options W/S, MCS WG, FFA Pre WCPFC meetings. Catch and Effort data which has the following resolution: * Longline 5°x5°/month and all flags combined * Purse seine 1°x1°/month and all flags combined
	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

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: Pending:

- MCS Working Group consultation and recommendation to FFC
- FFC approval

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 support the vision of the Regional MCS Strategy:

> *"An efficient and effective MCS framework in the Western and Central Pacific Ocean regional which supports the sustainable management of tuna resources and maximises the economic returns and social and development benefits, while minimising adverse environmental impacts*

RIMFS support member's efforts to detect IUU fishing risks and/or threats so that members are better able to prioritise, support and tailor MCS activities to prevent, deter and eliminate the IUU risk and/or threat through a combination of international and national responses.

RIMF provides FFA members the following services:

- a data warehouse and custodianship for the collection, storage, quality assurance and dissemination of MCS data;
- analysis and value-adding of MCS data and information to support MCS activities; and
- desensitizing information to facilitate sharing of MCS data.

2. Scope

The scope of *ISMS Policy Statement 3 – 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 and Surveillance Providers countries (AU, NZ, FR, and US). The high number of users and their diversity is a risk to be managed through uniform and universally agreed security standards.

Previous FFA member agreements or commitments to share MCS information is found in various locations, including but not limited to the Niue Treaty, FFC meeting records and bilateral arrangements. Information security risks regarding this MCS information arises 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 MCS 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 as Annex A to this Policy Statement. Variation to Annex A is by way of notification from either FFA Director of Fisheries Operations or Member's Official Contact.

Prior to RIMF access all users and administrators will agree to the following terms:

> *"It is a condition of [engagement type] with the Pacific Islands Forum Fisheries Agency that a I shall not communicate to any person, organization, government or to the press any unpublished information known to me by reason of my official position without obtaining prior permission of the Director-General at all times during and after termination of [engagement type, e.g. employment]."*

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

The FFA DG will accredit, by annex to this Policy, an area, room, group of rooms, buildings, or installation to be apart 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 B: Accredited RIMF Areas*.

5. Compliance

If any FFA employee is found to have breached this Information Security Policy, they may be subject to Disciplinary action.

Any violation of the policy by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.

Any violation of the policy by a Data User may result in suspension of data access privileges to a period of time as determined by the FFC.

Table 1: RIMF ACCESS & CONTROL

	Classified – High Red
RIMF Information Types	Fine scale catch and effort data. Compliance analysis for assigning a vessel's compliance index (Annex 2)
Access Control	Access and use will authorised to individuals authorised by: • DFO for FFA employees and agents with responsibility for RIMF Use or system administration; • Members Officials as provided under a Data Access Authorisation (*ISMS Policy Statement 1 – Data Access and Use Annex 3*) or similar documentation. • Members Officials will have access to all data "owned" by the Member Country
	Classified – Medium Yellow
Information Type	The RIMF portal will provide: • All attributes of vessels good standing on the FFA Vessel Register [1]; • Compliance Index of FFVs using *Annex B: Compliance Vessel Indexing*[2]; • RIMF Surveillance Picture where FFV VMS HS[3] and in-zone data, vessel's license details and compliance index are overlaid onto a mapping software program such as Google Earth[4]; and • Planning documents for Regional Surveillance Operations where the official is from an FFA Member country or a Surveillance Provider participating in the operation.
Access Control	*Electronically* A single login for the secure (https) internet portal for RIMF will be provided to a person designated by authorized MCS Entities and the FFA recognized Surveillance Providers of AU, NZ, FRA and US. The designated person will be responsible for managing the distribution and password of the login in a manner no less stringent than the FFA ISMS. The surveillance picture will be limited to those countries who have agreed to share VMS data with all other member countries, this may be time specific according to respective members' data sharing agreement. As of February 2012, this includes all members with the exception of AU, FJ, KIR, NZ and PNG. *Physical Access* Prior to physically accessing the the RIMF, member's Official Contact will provide the following information regarding individuals seeking access to the RIMF: name, position, affiliation, contact information, an explicit commitment to maintain a security standard no less stringent than the the FFA Security Information Management System.

[1] Authorised by FFC77 2011

[2] *Authorization by FFC to be confirmed by endorsement of this policy*

[3] *Authorization by FFC to be confirmed by endorsement of this policy*

[4] In-zone data of member countries who do not have a standing and ongoing agreement to share VMS will not be displayed (shared) on the Surveillance Picture.

Annex A: Register of RIMF Authorized Personnel and Entities

Name	Position & Rank	Organization
FFA RIMF User		
Mark Young	DFO	FFA
Lamiller Pawut	SOO1	FFA
Mike Pounder	SOO2	FFA
Ramesh Chand	MVMS	FFA
Allan Rahari	SOA	FFA
Fraser McEachan	MCSS	FFA
Apolosi Turaganivalu	CO	FFA
Steve Masika	VMSA	FFA
Daniel Koroi	VMSLO	FFA
Dennis Yehilomo	OMCSA	FFA
Ginia Harold	RDO1	FFA
Alisa Vavataga	RDO2	FFA
Henrietta Panda	VMSAA	FFA
Tim Park	OPM	FFA
Ambrose Orianihaa	AOPC	FFA
Fredrick Anii	OPC	FFA
FFA RIMF Administrators		
Nicklaus Reese	IT Manager	FFA
Henry Salonica	Network Administrator	FFA
Member Official RIMF User (required only for Classified High – Red material)		
MCS Entity (one person per entity, required for Classified Medium – Yellow material)		
Australia		
Required	Required	Australian Fisheries Management Authority (AFMA)
Required	Required	Australian Border Protection Command
Cook Islands		
Pamela Maru	Data Manager	Ministry of Marine Resources
Tuariki Henry (tuariki.henry@police.gov.ck	Commander Patrol Boat	Police Maritime Division
Federated State of Micronesia (FSM)		
Justino Helgen	VMS/Compliance Manager	National Oceanic Resource Management Authority (NORMA)
Nickolas Raifmai	VMS Officer	Police Maritime
Whylik Alfons	VMS Officer	Police Maritime
Fiji		
Meli Raicebe	VMS/Licensing Officer	Department of Fisheries, Ministry of Fisheries and Forest
Atunaisa Tawake	VMS Officer	Maritime Surveillance Centre, Royal Fiji Navy
Kiribati		
Taremon Korere	VMS Officer	Ministry of Fisheries & Marine

		Resources
John Mote	Officer Commanding Police Maritime	Kiribati Police Force & Prison
Marshall Islands		
Marcella Tarkwon	Compliance Officer	Marshal Islands Marine Resources Authority (MIMRA)
Ramon Kyle Aliven	Assistant MCS Officer	Marshal Islands Marine Resources Authority (MIMRA)
Required	**Required??**	Marshall Islands Sea Patrol
Nauru		
Ace Capella	MCS Officer	Nauru Fisheries Management Authority (NFMA)
Jeremiah Murin	VMS Officer	Nauru Fisheries Management Authority (NFMA)
New Zealand		
Dave Stevens	Analyst	Fisheries Communication Centre, Ministry of Fisheries
Niue		
Brendan Pasisi	Fisheries Director	Department of Agriculture, Forestry and Fisheries
Launoa Gatau	VMS/MCS Officer	Department of Agriculture, Forestry and Fisheries
Palau		
Thomas Tutii	OC Surveillance	Department of Maritime Law Enforcement
Required	Required	Bureau of Oceanic Fisheries
Papua New Guinea		
Bunu Mwatape	OIC	National Surveillance Coordination Centre (NSCC)
Samoa		
Yohni Fepuleai	VMS Officer	Ministry of Agriculture and Fisheries
Required	Required	Police Maritime Wing
Solomon Islands		
Charles Tobasala	VMS Officer	Ministry of Fisheries and Marine Resources
Charles Fox Sau	Operations Officer	Royal Solomon Islands Police Maritime Unit
Tokelau		
Feleti Tulafono	VMS/Licensing Officer	Department for Economic Development, Natural Resources & Environment
Tonga		
Ana Taholo	VMS/MCS Officer	Ministry of Agriculture, Food, Forest & Fisheries
Required	Required	Tongan Defense Services
Tuvalu		
Falasese Tupau	Fisheries Information and Licensing Officer	Department of Fisheries, Ministry of Natural Resources
Lopati Penihulo	VMS Officer	Department of Fisheries, Ministry of Natural Resources
Required	Required	Police Maritime Unit

Vanuatu		
Wesley Obed	Principal MCS Officer	Department of Fisheries
Tony Taleo	VMS/Licensing Officer	Department of Fisheries
Tari Tamata	Director	Vanuatu Police Maritime Wing
Surveillance Providers (one per provider)		
Required	Required	French Arm Forces French Polynesia (FAFP)
Required	Required	French Arm Forces New Caledonia (FANC)
Andrew Vanskike	Lieutenant	USCG Hawaii (District 14)
Richard Martin	Operations Officer (Intelligence)	NMCC, HQJFNZ
Robert Morris	SQNLDR	HQJOC, Australian Defense Force

Annex B: Accredited RIMF Areas

Accredited RIMF Area 1: The FFA Regional Fisheries Surveillance Centre.

The security measures of the FFA Regional Fisheries Surveillance Centre (RFSC) include:

Personnel Controls

- Access rosters listing persons authorized 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 RFSC.
- Non-MCS authorized personnel entering the RFSC must be continuously escorted by personnel authorised to be within the RFSC, during this time sensitive material will the secured.

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 RFSC perimeter walls, doors, windows, floors and ceiling, including all openings, provide sufficient sound attenuation to preclude inadvertent disclosure of conversation.
- The RFSC 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 RFSC entrance is limited to one door. A secondary door exists but is only used as an emergency exit.
- All RFSC 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 RFSC 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 RFSC primary entrance door is equipped with an automatic door closer and an access control device.
- The RFSC is located in a controlled area secured by two perimeter fences, each with controlled access points. The outer perimeter 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 RFSC 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 RFSC 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 RFSC due to an emergency condition or is an unauthorised MCS person.
- RFSC door construction is a solid wood core door, 144 millimetres thick.
- All vents, ducts, and similar openings that enter or pass through the RFSC 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.

Annex C: Compliance Indexing Vessels

The RFSC assigns each vessel listed on the FFA Record of Good Standing within the RIMF a compliance index using the criteria set out in *Table 1 - Vessel 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 iin-port Inspection reports; and
- Monitoring RFMO IUU lists

Table 1: **Vessel Compliance Index**

Index & Marker	Risk Level	Criteria
-5 Pulsating Large - Red	Non-Compliant	1. Vessel is on an RFMO IUU List; 2. Vessels is not on WCPFC Register of Fishing Vessels and is fishing for, or transshipping pelagic species in the High Seas; or 3. Vessel's Owner or Master is **known**[5] to have fished or is fishing in contravention of a national fisheries law or a Conservation and Management Measure (CMM) of an RFMO.
-4 Large - Red	Very High Risk of conducting IUU	1. Vessel Owner, Master or Beneficial Owner is **suspected** of fishing in contravention of a national fisheries law or a CMM of an RFMO; 2. Observer Report, Compliance Inspection Report or Compliance Analysis detected a known or **suspected** contravention of a national fisheries law or an RFMO's CMM in the last two years. 3. Vessel is not reporting VMS data as expected.
-3 Large - Orange	High Risk of conducting IUU	1. Vessel is on an NGO's IUU Blacklist; 2. Vessel has a position history of transiting EEZs where it is not licensed or is not the most direct route; or 3. Vessel has not had an observer onboard or a compliance inspection within last 2 years.
-2 Medium - Light Green	Medium Risk of conducting IUU	1. Vessel licensed for EEZ or HS in which it is operating and either an observer trip or compliance inspection was undertaken in the last 12 months; or 2. Vessel's has a position history of fishing adjacent to EEZs to which it is not licensed.
-1 Small - Light Green	Low Risk of conducting IUU	1. Vessel licensed for EEZ or HZ in which it is operating and an observer trip or compliance inspection was undertaken in last 12 months. Only minor or no infringement detected.

[5] Known is taken to be innocent until proven guilty under either national or international law .

ISMS Policy Statement 2: Human Resource Security

Document Details
Author: Fisheries Operations Division
Version: 1.0
Document Status: Pending:

- MCS Working Group consultation and recommendation to FFC
- FFC approval

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 – 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 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 has a role to play contributes to the safe and secure use of information and information systems FFA holds on behalf of its member countries.

3. Risks

FFA Secretariat holds sensitive information which may be put at risk if users do not follow the FFA 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

Through its orientation program, FFA shall ensure that all employees, contractors and third party users understand the FFA ISMS, their responsibilities related to it, are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

During employment and as part of FFA's ISMS implementation, FFA will ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error. All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

At termination of employment, contract or agreement, FFA shall ensure all employees, contractors and third party users return all organization 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

If any FFA employee is found to have breached this Information Security Policy they may be subject to Disciplinary action.

Any violation of the policy by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.

Annex A: Information Security Agreement for Employees & Contractors

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.

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 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)

I will not leave my computer unattended in such a state as to risk unauthorized 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 unauthorized 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 make myself familiar with FFA's Information Security Management System and its policies, procedures and any special instructions that relate to information security.

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.

I understand that if I breach any of the conditions listed above I may be subject to disciplinary action.

Name: ____-__

Position: ____

FFA Division: ____

Signature: __________________________________Date: ______________________

ISMS Policy Statement 3: Appropriate Use of E-mail

Document Details

Author:	Fisheries Operations Division
Version:	1.0
Document Status:	Pending:

- MCS Working Group consultation and recommendation to FFC
- FFC approval

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 – Appropriate Use of E-mail defines FFA policy concerned with the use of FFA e-mail accounts to ensure effective and appropriate use of FFA e-mail accounts in a manner which maintains the security of its information.

2. Scope

This policy applies to all staff and employees of FFA.

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 is provided to staff to assist them in carrying out their duties communicating efficiently and effectively with other staff members, other companies and partner organizations.

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 Users will comply with the following rules:

- Check e-mail daily to see if there are any messages;
- Include a meaningful subject line in all messages, check the address line before sending a message, check that it is being sent to the right person, and insert a signature block which includes name, position, phone and www.ffa.int;
- Delete e-mail messages when they are no longer required;
- Do not express views which could be regarded as defamatory or libelous;
- Do not print e-mail messages unless absolutely necessary;
- Do not expect an immediate reply as recipients might not be at their computer or could be too busy to reply straight away;
- Do not forward e-mail messages to others that were sent to you personally, particularly newsgroups or mailing lists, without the permission of the originator;
- Do not send excessively large e-mail messages or attachments;
- Do not send unnecessary messages such as festive greetings or other non-work items by e-mail, particularly to several or more people;
- Do not participate in chain or pyramid e-mail messages or similar schemes;
- Do not represent yourself as another person; and
- Do not use e-mail to send or forward material that could be construed as confidential, political, obscene, threatening, offensive or libelous.

A corporate e-mail filter is utilized to prevent e-mails being delivered which may contain inappropriate or malicious content. E-mails which need to be accessed to conduct FFA's business but are blocked can be made available by contacting the IT Help Desk. Authorization 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.

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.

Staff who utilize one of FFA's computers for personal use to send and receive e-mails must accept, as a condition of doing so, that their activity may be monitored.

Staff using FFA computers waives any rights to privacy regarding personal information on FFA's computers.

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.

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

Do not run software or click on a link to verify your 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. 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 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. Do not write anything about anybody that you cannot prove and evidence.

5. Compliance

If any FFA employee is found to have breached this Information Security Policy, they may be subject to Disciplinary action.

Any violation of the policy by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.

ISMS Policy Statement 5: Information Backup

Document Details
Author: Fisheries Operations Division
Version: 1.0
Document Status: Pending:

- MCS Working Group consultation and recommendation to FFC
- FFC approval

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 policy and strategy for backing up the organisation's information and software application systems. The aim is to ensure that it is always possible to recover the 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

Backup Method

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.

Backup and Restore Procedures

The servers and systems will be backed up using the standard facilities available within the backup software being used.

Documentation with sufficient detail to allow an experienced user of the backup software to restore data will be maintained.

Backup Status

Backup software will be configured to automatically alert an administrator as to the status of any backup performed.

Backup status will be reviewed on a daily basis and any faults identified will be rectified.

Verification and Restore Testing

Where possible the backup software will be configured to automatically verify the backup. The verification will be accomplished by comparing the contents of the backup to the data on disk.

The restoration of information from backup will be tested periodically.

Backup Cycles

Data Repository - Where possible a full backup of important systems will be taken every day. If there is insufficient available time to perform a full backup, then at a minimum a full backup will be taken weekly, with incremental backups being taken every day.

Daily Backups - Daily backups will consist of backup taken every day as part of a simple daily rotation or as part of a GFS rotation scheme.

Daily backups consist of either a full backup or an incremental / differential backup.

Weekly backup will consist of a full backup.

Monthly Configuration Backup - Monthly configuration backups will consist of exporting or backing up the configuration settings of an application. The configuration will be stored on a server that is backed up daily.

Backup Storage

Backup media will be securely stored when not in use.

Online and remote disk mirroring backups will be held at a data centre at least [2] km away from the data centre containing the information being backed up.

For resilience several removable media will be stored off site.

A schedule for off site storage will be logged.

Application Backup

Use will be made of online backup techniques when they are available to minimize downtime.

Full offline backups will be utilised where online backups are not available.

Backup Guidelines

The backups of servers and applications will at a minimum comply with the following guidelines.

Server / Application	**Backup Cycle**	**Media**
Unix Apps Server	Daily	NAS
Active Directory Server	Daily	NAS
Windows File Server	Daily	NAS
Database Servers	Daily	NAS
Application Server Data	Daily	NAS
Application Server	Daily	NAS
DMZ Server	Weekly	NAS
Test Server	As appropriate	NAS
Firewall	Monthly Configuration	NAS
Internet Gateway	Monthly Configuration	NAS
Network Switches	Monthly Configuration	NAS
VoIP Servers	Monthly Configuration	NAS
Satellite Modems	Monthly Configuration	NAS

2. Backup Media Type:

1. Network Attached Storage (NAS)
2. Secure Online Data Sync

3. Servers and folders backed up

- FFA Databases: Spearfish:/home/backups/database
- FFA User home drives: mackerel2://srv/smb/homes/FFA/
- FFA Shared folders: mackerel2://srv/smb/files/
- FFA achieves: mackerel2://srv/smb/archive

4. Honiara Backup Schedules

- Weekly backup on NAS spearfish2
- Monthly backup on NAS FFA-NAS-backup

5. Compliance

If any member of IT staff is found to have breached this policy, they may be subject to disciplinary action.

Any violation of the policy by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.

ISMS Policy Statement 6: INFRASTRUCTURE HARDENING

Document Details
Author: Fisheries Operations Division
Version: 1.0
Document Status: Pending:

- **MCS Working Group consultation and FFC recommendation**
- **FFC approval**

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 can not 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

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.

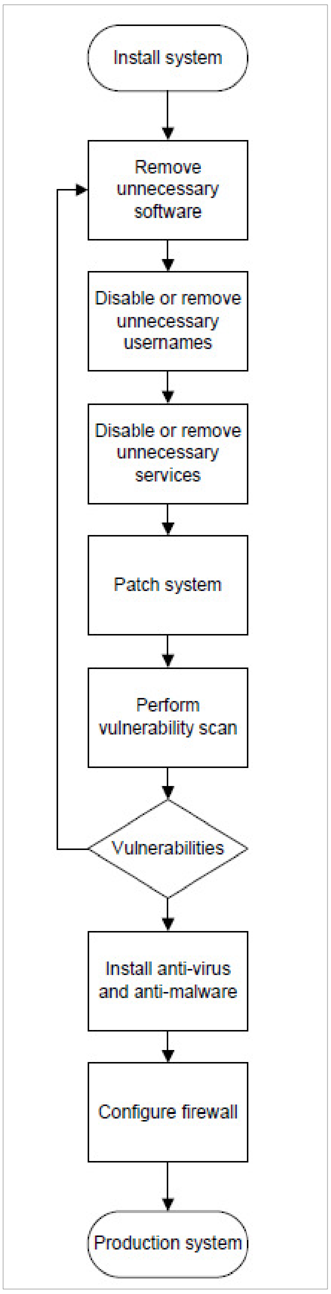
If external systems such as web servers and e-mail servers advertise their type and version, it makes it easier for an attacker to exploit known weaknesses.

Systems which run unnecessary services and have ports open which do not need to be open are easier to attack as the services and ports offer opportunities for attack.

4. Policy

Hardening Process

All new systems will undergo the following hardening process:


Install system
Remove unnecessary software
Disable or remove unnecessary usernames
Disable or remove unnecessary services
Patch system
Perform vulnerability scan
Vulnerabilities
Install anti-virus and anti-malware
Configure firewall
Production system

- Install System – Systems will be installed as per the vendor's instructions.

- Remove Unnecessary Software - Most systems come with a variety of software packages to provide functionality to all users. Software that is not going to be used in a particular installation will be removed or uninstalled from the system.

- Disable or Remove Unnecessary User Names - Most systems come with a set of predefined user accounts. These accounts are provided to enable a variety of functions. Accounts relating to services or functions which are not used will be removed or disabled. For all accounts which are used the default passwords will be changed. Consideration will be given to renaming predefined accounts if it will not adversely affect the system.

- Disable or Remove Unnecessary Services - All services which are not going to be used in production will be disabled or removed.

- Patch System - The system should be patched up to date. All relevant service packs and security patches will be applied.

- Perform Vulnerability Scan - The system will be scanned with a suitable vulnerability scanner. The results of the scan will be reviewed and any issues identified resolved.

- Vulnerabilities - If there are no significant vulnerabilities the system can be prepared for live use.

- Install Anti-Virus and Anti-Malware - A suitable anti-virus and anti-malware package will be installed on the system to prevent malicious software introducing weaknesses in to the system.

- Configure Firewall – When the FFA system runs its own firewall suitable rules will be configured on the firewall closing all ports not required for production use.

- The system is now ready for production use.

Hardening Requirements

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.

Vulnerability scanning and inventory scanning software will be configured to automatically uninstall unauthorized software.

BIOS passwords will be implemented on all PCs and laptops to protect against unauthorized changes.

The boot order of PC's and laptops will be configured to prevent unauthorized booting from alternative media.

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.

Default passwords will be changed following installation and before use in a production environment.

All PC's and servers will be protected by anti-virus and anti-spyware software. The anti-virus and anti-spyware software will be configured to automatically download the latest threat databases.

A local firewall will be installed on all PC's and laptops. The firewall will be configured to only allow incoming traffic on approved ports and from approved sources.

The use of removable media will be controlled by endpoint protection software.

All servers must pass a vulnerability assessment prior to use. The servers will be scanned using FFA's vulnerability scanning tools. All network and operating system vulnerabilities will be rectified prior to use.

Public facing servers will be further hardened by obfuscation. The headers on web servers and e-mail servers will be changed so that it is not immediately apparent what software they are running.

All devices on FFA's network will be scanned for vulnerabilities every three months. Any issues identified will be reviewed and rectified as appropriate.

All devices on FFA's network will patched as soon as patches become available from the vendor.

5. Compliance

If any FFA employee is found to have breached this Information Security Policy they may be subject to Disciplinary action.

Any violation of the policy by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.

ISMS Policy Statement 7: Appropriate use of Internet

Document Details
Author: Fisheries Operations Division
Version: 1.0
Document Status: Pending:

- MCS Working Group consultation and recommendation to FFC
- FFC approval

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 minimize security exposure of FFA's information and information systems to the internet.

2. Scope

This policy applies to all FFA staff and employees.

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.

Occasional and reasonable personal use of the internet is permitted in your own time subject to the conditions set out in FFA ISMS. When using FFA's internet access facilities, Users will comply with the following guidelines and rules:

- Keep use of the internet to a minimum;
- Check that any information accessed on the internet is accurate, complete and current;
- Check the validity of the information found;
- Respect the legal protections to data and software provided by copyright and licenses;
- Inform FFA IT Helpdesk (helpdesk@ffa.int) immediately of any unusual occurrence;
- Do not visit any website that is perceived to be potentially offensive, this will include websites with pornographic, racist, sexist, ageist, homophobic, content or websites that promote religious hatred;
- Do not download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity;
- Do not download software from the Internet and install it upon FFA's computer equipment;
- Do not use FFA's computers to make unauthorized entry into any other computer or network;
- Do not disrupt or interfere with other computers or network users, services, or equipment;
- Note that intentional disruption of the operation of computer systems and networks is a crime;
- Do not represent yourself as another person;
- Do not use internet access to transmit confidential, political, obscene, threatening, or harassing materials; and
- Do not publish or post defamatory or libelous material.

A corporate internet filter is utilized 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. Authorization 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.

Monitoring of Internet usage

All content viewed is scanned for viruses and offensive material.

Use of the internet is recorded and may be monitored. It is possible to identify Internet sites visited by individual users.

FFA reserves the right to inspect any files at any time during an investigation where there is suspected misuse and to withdraw access to the internet.

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.

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.

Staff using FFA computers waives 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.

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

The playing of internet computer games is not allowed.

Using the Internet for personal purposes must comply with the principles set out in this FFA ISMS.

Software uploads and downloads

FFA has a corporate standard desktop system. Staff is not allowed to download programs or software (including screen savers and wallpaper) from the internet including programs or software available for trial purposes.

If programs or software available on the Internet are required for a genuine business need, staff must produce a business case and contact the IT Department who will make the necessary arrangement to acquire and arrange for the installation of the programs or software.

Purchasing of goods and services

The purchasing of goods or services via the Internet is subject to FFA's financial procedures. These must be consulted to determine which goods and services it is permissible to purchase.

Participation in public Internet forums

An internet forum is a web application for holding discussions and posting user generated content. Internet forums are also commonly referred to as Web forums, message boards, discussion boards, discussion forums, bulletin boards, or simply forums.

The use of work related Internet forums for professional or technical purposes is permitted.

You must make every attempt to avoid bringing FFA's name into disrepute or to adversely affect its reputation, customer relations or public image.

Personal use of public internet forums should not be conducted using FFA's IT equipment.

Computer viruses and malicious programs

Computers can be infected by viruses and malicious programs by just visiting a webpage.

If you think you have a computer virus report it to the FFA IT Helpdesk immediately.

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

If any FFA IT staff or FFA internet user is found to have breached this policy, they may be subject to disciplinary action.

Any violation of the policy by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.