6TH MEETING OF THE FINANCE AND ADMINISTRATION COMMITTEE (FAC)

The Hague, The Netherlands, 23 to 27 January 2019

FAC 6 - Doc 11

The Secretariat's Internal Data and Security Procedures

Secretariat

South Pacific Regional Fisheries Management Organisation
PO Box 3797, Wellington 6140, New Zealand.
T: +64 4 499 9889 - F: +64 4 473 9579 – E: secretariat@sprfmo.int

Table of Contents

1. Background

At the 6th Meeting of the Commission held at Lima, Peru, the Commission advised the Secretariat *"to develop in consultation with the CTC (Compliance and Technical Committee) Chair an internal electronic data and communication security procedures." (COMM 6 – Report – ANNEX 8c: Secretariat Security Standards for the Use of the Commission Data)*

As guided by the Commission, this document covers: Disaster Recovery Plan and Procedures, Prevention of network compromise, Prevention of data compromise and Prevention of data loss.
This document has been prepared in consultation with the CTC Chair, who has approved it after having consultative meetings with the Secretariat.

2. Internal Electronic Data and Communication Security Procedures

A. Disaster Recovery Plan and Procedures

Information Technology Statement of Intent

This document delineates SPRFMO's policies and procedures for technology disaster recovery, as well as the process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes the recommended procedures. In the event of an actual emergency, modifications to this document may be made to ensure the physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

Policy statement

The Secretariat has agreed upon the following policy statement:

- The organisation shall develop a comprehensive IT Disaster Recovery Plan (DRP).
- The DRP should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- All staff must be made aware of the DRP and their own respective roles.
- The DRP is to be kept up to date to consider changing circumstances.

Objectives

The principal objective of the DRP is to develop, test and document a well-structured and easily understood plan which will help the organisation recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan.
- The need to ensure that operational policies are adhered to within all planned activities.
- The need to ensure that proposed contingency arrangements are cost-effective.

Staff contact info

Name, Title	Contact Option	Contact Number
Sebastian Rodriguez,	Work	+64 4 499 9889
Executive Secretary	Mobile	+64 21 0267 9400
	Email Address	srodriguez@sprfmo.int
Craig Loveridge,	Work	+64 4 499 9894
Data Manager	Mobile	+64 27 272 6252
	Email Address	cloveridge@sprfmo.int
Yanbin Liu,	Work	+64 4 499 9885

Name, Title	Contact Option	Contact Number
Finance and Office Manager	Mobile	+64 221272650
	Email Address	yliu@sprfmo.int
John V K Cheva,	Work	+64 4 499 9886
IT & VMS Manager	Mobile	+64 21 125 1152
	Email Address	jcheva@sprfmo.int
Susana Delgado,	Work	+64 4 499 9893
Coordination and Communications Officer	Mobile	+64 21 115 1869
	Email Address	sdelgado@sprfmo.int
Jongkwan Ahn	Work	+64 4 499 9890
Seconded Fishery Officer	Mobile	+64275983046
	Email Address	jahn@sprfmo.int

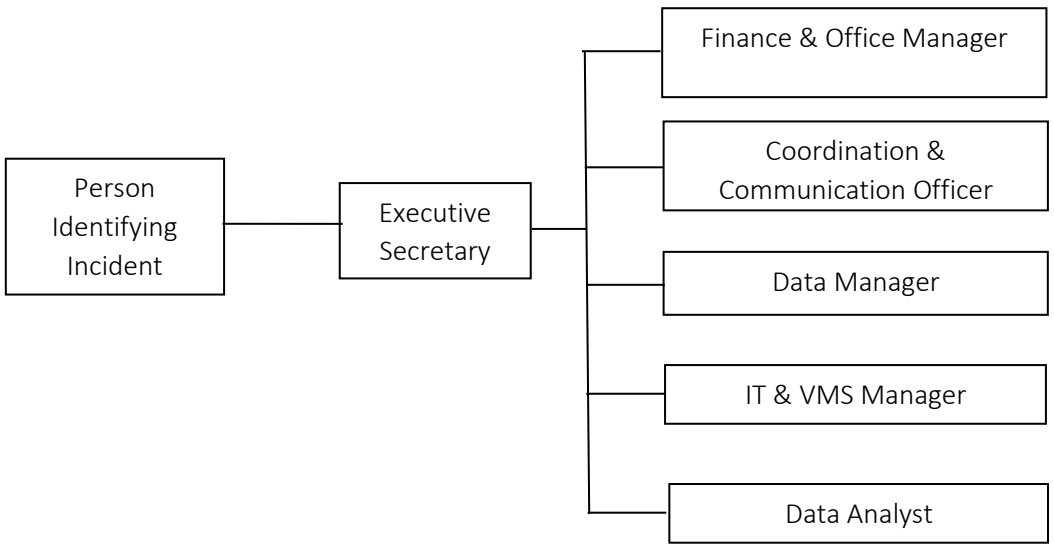
Temporary Personnel Under Contract

Marianne Vignaux	Work	+64 4 499 9889
Data Analyst	Mobile	+64 223199039
	Email Address	analyst@sprfmo.int

External Contacts

Name, Title	Contact Option	Contact Number
Landlord/Property Manager	CBRE	
	Work	0800 227 332
	Email Address	pulseresponse@cbre.co.nz
Power Company		
Account Number 100 121 7387	Work	0800 600 900
	Email Address	business@genesisenery.co.nz
Telecom Carrier		
Account Number 300985033	Work	126; 0800 287 463
	Email Address	Daniel.braines@hubwellington.co.nz

Notification Tree



Emergency Response Team (ERT)

Members of the ERT are:

- Sebastian Rodriguez - Executive Secretary
- John Cheva - IT & VMS Manager
- Craig Loveridge - Data Manager

Disaster Recovery Team

The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish facilities for an emergency level of service within 2 business hours;
- Restore key services within 4 business hours of the incident;
- Recover to business as usual within 8 to 24 hours after the incident;
- Coordinate activities with disaster recovery team, first responders, etc.
- Report to the emergency response team.

1) Plan Overview

a) Plan Updating

It is necessary for the DRP updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the plan. This will involve the use of formalized change control procedures under the control of the IT Manager.

b) Plan Documentation Storage

Each member of the staff will be emailed a copy of the plan. They will also be issued a USB stick and hard copy of this plan to be filed at home. A master copy will be stored in the bank locker procured for the purpose of storing data backup in an offsite location.

c) Backup Strategy

Key business processes and the agreed backup strategy for each are listed below.

KEY BUSINESS PROCESS	BACKUP STRATEGY
Organisation data (Files & Folders)	Cloud, on-site & Off-site data storage facility

d) Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency has been examined. The focus here is on the level of disruption which could arise from each type of disaster.
Potential disasters have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Brief Description of Potential Consequences & Remedial Actions
Earthquake	2	3	Damage to the building resulting in being stopped to enter the building until the clearance to enter is awarded by the structural engineers. Building earthquake resilient certified.
Flood	5	5	All critical equipment is located on the 26th Floor.
Fire	3	4	Fire and smoke detectors on all floors.

Tsunami	3	4	Being on the 26th floor should be OK, but access to work via the CBD could possibly be affected.
Electrical storms	5	4	Electrical surge protection available on the uninterrupted power supply (UPS).
Act of sabotage	5	4	Access to the office is through one door which is only accessible through a security card.
Electrical power failure	3	4	UPS with surge protection to the shut the server safely that is tested fortnightly and monitored.
Loss of communications network services	4	4	Unable to connect to the SPRFMO network. Inform the service provider.
Cyber attack	4	2	Unable to use the email. Strengthening of the anti-spam, anti-phishing and anti-spoofing policies.

Probability: 1=Very High, 2=High, 3=Medium, 4=Low, 5=Very Low

Impact: 1=Total destruction, 2= Substantial/Considerable destruction, 3=Partial destruction, 4= Minor disruption, 5= No disruption

According to the Wellington Region Emergency Management website, "If you feel an earthquake that is either longer than a minute OR strong enough that it's hard to stand up, as soon as the shaking stops, get to high ground, out of all zones (past the blue line)! If there is an official warning, then evacuate from the zones (red, orange or yellow) is stated in the warning."

If there is an official warning, then evacuate from the zones (red, orange or yellow) stated in the warning.

The **Red Zone** is the beach and marine environment, and some very low-lying areas. This zone is the one where people are asked to stay out of most often as a result of smaller tsunamis.

The **Orange Zone** (including the red zone) is the area which may be evacuated for large earthquake in the Pacific, such as near South America, causing a tsunami wave of up to 5 metres at the Wellington coastline. Alerts and evacuation advice would be issued by Civil Defence and distributed to the public for this type of tsunami.

The **Yellow Zone** (including the orange and red zones) is the area that must be evacuated from if a long or strong earthquake is felt.

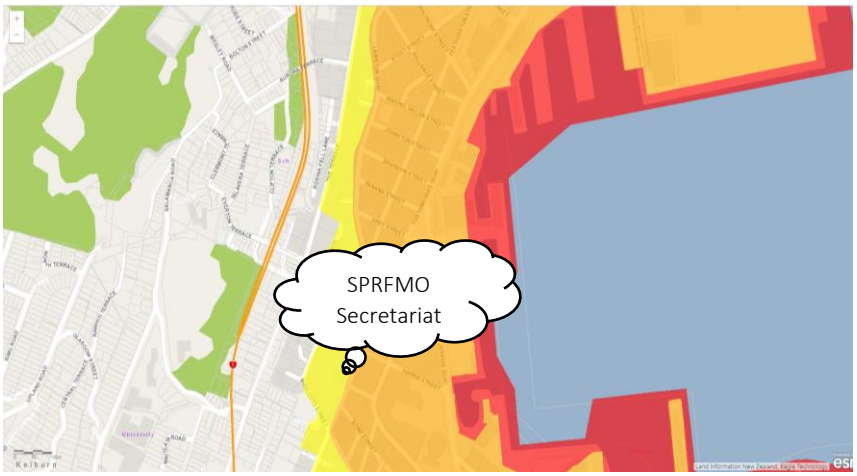


Figure 1 SPRFMO Secretariat's location

2) *Emergency Response*

a) Alert, escalation and plan invocation

i) Plan Triggering Events

Key trigger issues at Secretariat that would lead to activation of the DRP are:

- Total loss of data
- Total loss of all communications
- Total loss of power
- Loss of the building

ii) Activation of Emergency Response Team

When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees must be issued a Quick Reference card (Annex 1) containing ERT contact details to be used in the event of a disaster.

Responsibilities of the ERT are to:

- Respond immediately to a potential disaster and call emergency services;
- Assess the extent of the disaster and its impact on the organisation, data centre, etc.;
- Decide which elements of the DRP should be activated;
- Establish and manage a disaster recovery team to maintain vital services and return to normal operation;
- Ensure employees are notified and allocate responsibilities and activities as required.

b) Emergency Alert, Escalation and DRP Activation

This policy and procedure have been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted.

The DRP will rely principally on key members of the staff who will provide the technical and management skills necessary to achieve a smooth technology and organisation recovery. Suppliers of critical goods and services will continue to support the recovery of operations as the organisation returns to normal operating mode.

i) Emergency Alert

The person discovering the incident calls a member of the Emergency Response Team in the order listed:
Emergency Response Team

- Executive Secretary
- IT & VMS Manager
- Data Manager

If not available, try:

- Finance & Office Manager
- Coordination & Communications Officer
- Data Analyst

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the organisation's capability to perform normally.

3) *Insurance*

As part of the organisation's disaster recovery, the SPRFMO Secretariat has an insurance policy has been put in place. This includes general liability, statutory liability, material damage and business interruption.

Policy Number	Policy Name	Coverage Type	Coverage Period	Amount of Coverage	Next Renewal Date
6000124911	Material Damage	Contents	9th May 2018 to 9th May 2019	$17,500	9th May 2019
	General Liability	-		NZ$10,000,000	
	Statutory Liability	-		NZ$1,000,000	

B. Prevention of network compromise

Access to Secretariat's network

Only authorised staff members of the Secretariat have access to the Secretariat's network. Each one of them have been issued a password following the password policy as mentioned below:

Password Policy

Enforce Password History	24 passwords remembered
Maximum password age	180 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled

Anti-Virus

The server is protected by a firewall (windows) to deter any unauthorised intrusion into the organisation's network.

ANTI-VIRUS	
ESET ENDPOINT	Individually installed on 8 client machines and 1 server
ESET REMOTE ADMINISTRATOR	Installed on the server to remotely install and deploy updates on the client machines.

Software updates & monitoring of alerts

All software updates are monitored through the ESET Remote Administrator and updated on a weekly basis. Windows updates are scheduled to be carried out after office hours. Server updates are scheduled to be carried out on the weekends remotely by the system administrator.

Alerts for software updates (system and Office 365) are configured to notify the system administrator. Once notified, the software updates are deployed either as a group or individually. The deployment status is monitored.

A daily health report of the server and the clients is sent to the administrator daily at 3 a.m. providing information on:

- Critical alerts and warning:
- Critical errors in the event logs:
- Server backup:
- Auto-start services not running:
- Updates:
- Storage:

In addition, a real-time report from the printer/scanner/copier is sent to the administrator, informing of any errors or failures that may prevent the staff from using the printer/scanner/copier.

Service Level Agreements (SLA)

Service Provider	Service Provided
Need a Nerd	Daily (SPRFMO server files and folders) and weekly back-up (SPRFMO archive folder) using the Keep It Safe Online Backup International Services software.
IT Engine	Onsite back-up of data using Storage Craft Shadow Protect SPX software
CLS	THEMIS (Commission VMS) software support and maintenance to provide 99.7% fault tolerance
FINNZ	Vessel licence and Catch Data Management

C. Prevention of data compromise (Secretariat's Mobile Device Acceptable Use Policy)

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for SPRFMO staff members who have legitimate business requirements to use a private or SPRFMO provided mobile device that can access the organisation's electronic resources. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/Notebook
- Tablet computers such as iPads
- Mobile/cellular phones
- Smartphones
- PDAs
- Any mobile device capable of storing data and connecting to a network.

This policy is developed to protect the integrity and confidential data that resides within the Secretariat's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be compromised. A breach of this type could result in loss of information, damage to critical applications, financial loss, and damage to the SPRFMO's public image.

Applicability

Threat	Description
Loss	Devices used to transfer, or transport work files could be lost or stolen.
Theft	Sensitive data is deliberately stolen and sold by an employee.
Copyright	Software copied onto a mobile device could violate licensing.
Malware	Viruses, Trojans, Worms, Spyware and other threats could be introduced via a mobile device.

This policy applies to all Secretariat employees, including full and part-time staff, contractors and

other agents who utilize either Secretariat-owned or personally-owned mobile device to access, store, back up, relocate or access any SPRFMO's resources/info. Consequently, employment at Secretariat does not automatically guarantee the initial and ongoing ability to use these devices to gain access to Secretariat's networks and information.

The policy addresses a range of threats:

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of the IT Manager. Unauthorized use of mobile devices to back up, store, and otherwise access any SPRFMO related information/data is strictly forbidden.

Policy and Appropriate Use

It is the responsibility of any employee of Secretariat who uses a mobile device to access Secretariat's resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct Secretariat business be utilized appropriately, responsibly, and ethically.

Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

1) Access Control

a) The Secretariat reserves the right to refuse the ability to connect mobile devices to Secretariat and Secretariat's-connected infrastructure. The Secretariat will engage in such action if it feels such equipment is being used in such a way that puts the Secretariat's systems, data, and staff at risk.

b) Prior to initial use on the Secretariat's network or related infrastructure, all mobile devices must be registered with the Secretariat**.** The Secretariat's IT Manager will maintain a list of approved mobile devices and related software applications and utilities as needed. Devices that are not on this list may not be connected to Secretariat's infrastructure.

c) SPRFMO staff members who wish to connect such devices to non-Secretariat's network infrastructure to gain access to Secretariat data must employ, for their devices and related infrastructure, security measures deemed necessary by the Secretariat such as updated software, anti-virus software, and personal firewall.

All mobile devices attempting to connect to the Secretariat's network through a network (i.e. the Internet) will be inspected using technology centrally managed by Secretariat's IT Manager. Laptop computers or personal PCs may only access the Secretariat's network using an SPRFMO Virtual Private Network (VPN) connection which will be configured by the IT Manager.

2) Security

a) SPRFMO staff members using mobile devices and related software for network and data access will, without exception, use secure data management procedures**.** All mobile devices must be protected by a strong password. Employees agree to never disclose their passwords to anyone**.**

b) SPRFMO staff are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain Secretariat data. Any non-Secretariat computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by Secretariat's IT Manager. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.

c) Employees, contractors, full time, part time and temporary staff will permanently erase Secretariat-specific data from such devices once their use is no longer required.

d) In the event of a lost or stolen mobile device, it is incumbent on the user to report this to Secretariat immediately. The device will be removed from the list of Secretariat's registered devices and disconnected from accessing the network of the Secretariat. If the device is recovered, it can be submitted to the Secretariat for re-provisioning.

e) Employees, contractors, full time, part time and temporary staff will make no modifications of any kind to Secretariat-owned and installed hardware or software without the approval of the IT Manager. This includes, but is not limited to, any reconfiguration of the mobile device.

3) Organizational Protocol

The end user agrees to and accepts that his or her access and/or connection to Secretariat's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains the Secretariat's highest priority.

4) Policy Non-Compliance

Failure to comply with the Mobile Device Acceptable Use Policy may result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment in accordance to Regulation 10.4 (Gross dereliction of duties) of SPRFMO Staff Regulations.

D. Prevention of data loss

Backup Plan for data on the server

OVERVIEW	
SERVER	**Location:** 26th Floor, Plimmer Towers, 2-6 Gilmer Terrace, Wellington **Year of purchase:** 2013 **Server Model:** HP X64 Class PC (ProLiant ML3 10e Gen8) **Operating System:** Microsoft Windows Server 2012 Essentials CPUs: Intel® Xeon® CPU E3-1220 V2 @ 3.10GHz, 3100 MHz, 4 Core(s), 4 Logical Processors **Memory:** 8.00 GB **Total Disk:** 464 GB **System Serial #:** AUD32302F3 **IP Address:** 10.10.5.1 **DNS Entry:** SPRFSVR.SPRFDOM. local
Uninterrupted Power Supply (UPS)	Dynamix UPSD1600 Defender 1600VA (960W) Line Interactive UPS, 3x NZ Power Sockets with Surge + Battery Backup, 3x NZ Power Sockets with Surge 936J Netguard Smart Monitoring

BACKUP STRATEGY	
Hourly	Onsite (NAS (wgtn-nas) – Intel® Celeron® N3160 @ 1.60GHz (4 cores)) using Storage Craft Shadow Protect SPX software
Daily	Keep It Safe Online Backup International Services (http://www.keepitsafe.co.nz/dr)
Weekly	The archive folder is backed-up using the Keep It Safe Online Backup International Services
Monthly	Off-site storage of backup data (copied to an external Hard-Disk) in a bank locker
Monthly	Onsite backup of system files using Windows Server Backup tool to an external Hard-Disk.

SYSTEM DISASTER RECOVERY PROCEDURE	
Total Loss of Data	The entire data can be recovered from one or several sources of backup as mentioned in the Backup Strategy.
Total Loss of System Files	The entire system can be recovered from the backup (external Hard-Disk).

Staff training on storage of data

The Secretariat staff is trained to store all data relating to SPRFMO in the relevant folders on the server. They are also trained to retrieve data from backup.

E. Case Study

On 9th November 2018, the Communication and Coordination Officer identified that the Secretariat's sent email box contained emails that were sent by somebody using the email address of the Secretariat. This kind of attack is known as 'spoofing'. As a preventive measure, Office 365 blocks an email box once a large number of emails are continuously sent from it. This resulted in blocking of the Secretariat's email sending capability.

The Communication & Coordination Officer informed about the incident to the IT & VMS Manager (as per Para 2.2.1 Emergency Alert). As the Executive Secretary was attending a meeting outside the office premises, the IT & VMS Manager was informed (as per Para 2.1.1 Plan Triggering Events). Once the Executive Secretary came back to the office, he was informed of the attack. The Executive Secretary and the IT & VMS Manager formed the Disaster Recovery Team and came up with strategies to stop this attack (as per Para 2.1.2 Activation of Emergency Response Team).

Considering the damage such an attack could cause, a ticket was raised immediately with Microsoft Office 365 to rectify the problem. A support technician immediately responded. The Anti-phishing policy was adjusted to stop any further spoofing attack.

The Secretariat's email sending feature was unblocked in the settings and a request was placed with Office 365. After unblocking the email box, a test email was sent and was confirmed that the receiver received the test email.

The whole process was brought under control within a couple of hours since the attack was detected (as per one of the responsibilities of the Disaster Recovery Team).

3. ANNEX 1 – EMERGENCY RESPONSE TEAM (ERT) CONTACT DETAILS

Name, Title	Contact Option	Contact Number
Sebastian Rodriguez,	Work	+64 4 499 9889
Executive Secretary	Mobile	+64 21 0267 9400
	Email Address	srodriguez@sprfmo.int
John V K Cheva,	Work	+64 4 499 9886
IT & VMS Manager	Mobile	+64 21 125 1152
	Email Address	jcheva@sprfmo.int
Craig Loveridge,	Work	+64 4 499 9894
Data Manager	Mobile	+64 27 272 6252
	Email Address	cloveridge@sprfmo.int