AD HOC TASK GROUP
[DATA]
31 July - 4 August 2006
Manila, Philippines

DRAFT INFORMATION SECURITY POLICY

WCPFC/AHTG [Data]/2006/07

Paper prepared by the Secretariat

1. The Second Session of the Commission adopted a recommendation to establish an ad hoc Task Group [AHTG] (Data) to identify types of data that must be treated as confidential and to develop draft rules and procedures to govern the security and confidentiality of data collected and held by the Commission.

2. In support of the work of the AHTG (Data), the Secretariat, in collaboration with members of the Scientific Committee's Statistics Specialist Working Group (S-SWG), circulated the following draft documents on 6 April 2006 for comment:

- Draft Rules and Procedures for the Security of Data held by the WCPFC;
- Draft Principles and Procedures for Dissemination by the Commission of Fisheries Compliance Data; and
- Draft Principles and Procedures for the Dissemination of Scientific Data by the Commission.

3. Comments on the above drafts received from Members by 31 May 2006 included a recommendation that the AHTG (Data) should also consider an overarching Information Security Policy that would support the above rules, principles and procedures. The attached document (Appendix A) has been prepared in response to that recommendation for the consideration of the AHTG (Data).

Appendix A

DRAFT
INFORMATION SECURITY POLICY
Version 1.0
[July 2006]

Western and Central Pacific Fisheries Commission
PO Box 2356
Kolonia 96941
Pohnpei State
Federated States of Micronesia

WESTERN AND CENTRAL PACIFIC FISHERIES COMMISSION

INFORMATION SECURITY POLICY
[Draft]
[July 2006]

Table of Contents

WESTERN AND CENTRAL PACIFIC FISHERIES COMMISSION

INFORMATION SECURITY POLICY
[Draft]
[July 2006]

1. PURPOSE

Information is the basis on which the Western and Central Pacific Fisheries Commission (WCPFC) Secretariat conducts its business. As the custodian of a large volume of information on behalf of Members, Cooperating Non-members and Participating Territories that is either commercially, personally or politically sensitive, the Secretariat has a fundamental responsibility to protect that information from unauthorized or accidental modification, loss, release or impact on the safety and well-being of individuals, Commission Members, Participating Territories and Cooperating Non-members. In addition, information of assured quality must be available to undertake the Secretariat's day to day business on behalf of the Commission.

The purpose of this Information Security Policy is to enunciate the Secretariat's direction and support for information security. This Policy sets a clear direction, and demonstrates support for, and commitment to the management of information security at all levels of the Commission.

2. CONTEXT

This Policy has been developed by the WCPFC Secretariat. It will be complemented by a variety of other documents describing policies, procedures, guidelines and controls with regard to specific aspects of information security management in the Commission.

Together the policies, procedures, guidelines and controls will form an Information Security Plan which commits the management and staff of the WCPFC Secretariat to best practice for information security management.

3. GOALS AND OBJECTIVES

The goal of information security is to protect the WCPFC Secretariat from adverse impact on its reputation and operations that could result from failures of:

- *Confidentiality* in the context of access or disclosure of the information without authority;
- *Integrity* - in the context of completeness, accuracy and resistance to unauthorized modification or destruction;
- *Availability* - in the context of continuity and the business processes and for recoverability in the event of a disruption.

The objectives of this Policy are to:

- Support the efficient use of human, financial and information resources in the WCPFC Secretariat to deliver best practice information services to Members, Participating Non-members, Cooperating Non-members and other stakeholders in the WCPFC;
- Minimise the possibility of a threat to information security causing loss or damage to the WCPFC Secretariat, its Members, Participating Territories and Cooperating Non-members and other stakeholders;
- Minimise the extent of loss or damage from a security breach or exposure;
- Ensure that adequate resources are applied to implement an effective information security program;
- Identify the essential measures of the information security program;
- Inform all the WCPFC Secretariat personnel, Members, Participating Territories, Cooperating Non-members and other stakeholders who have access to the WCPFC Secretariat information of their responsibilities and obligations with respect to information security;
- Ensure that the principles of information security are consistently and effectively applied during the planning and development of the Secretariat's activities.

4. SCOPE

This Policy applies to:

- All users of WCPFC Secretariat information including service providers to the Secretariat;
- All information assets including facilities, data, software, paper documents and personnel.

Facilities include:

- Equipment, as well as the physical and environmental infrastructure;
- Computer processors of all sizes, whether general or special purpose, including personal computers;
- Peripheral, workstation and terminal equipment;
- All forms of electronic storage media
- Telecommunications and data communications cabling and equipment;
- Local and wide area network equipment;
- Environmental control systems, including air-conditioning and other cooling equipment;
- Alarms and safety equipment;
- Required utility services, including electricity, gas and water;
- Buildings and building improvements accommodating personnel and equipment.

Data includes:

- Raw and processed data:
- Electronic data files, regardless of their storage media and including hard copies and data otherwise in transit;

- Information derived from processed data, regardless of the storage or presentation media.

Software includes:
- Locally developed programs and those acquired from external sources:
- Operating system software and associated utility and support programs;
- Application enabling software, including data base management, telecommunications and networking software;
- Application software.

Paper documents includes:
- Technical reports, systems documentation, user manuals, continuity plans, contracts, guidelines and procedures.

Personnel includes:
- Employees, contractors, consultants, service providers, representatives of Members, Participating Territories, Cooperating Non-members and other stakeholders that access the Secretariat's information and data.

5. RESPONSIBILITIES

The Executive Director is the person responsible for the administration of internal processes to implement this Policy and the accompanying Plan. Periodic monitoring, review and evaluation will ensure best practice for information security is maintained in response to changes in the WCPFC business environment.

The Executive Director will co-ordinate the development of the policies, procedures, guidelines and controls which together will form an Information Security Plan (see framework at Appendix A).

The Executive Director will be responsible for an on-going review of the effectiveness of the policies, procedures, guidelines and controls described in the plan.

The Executive Director will ensure that all Secretariat personnel are fully informed of their obligations and responsibilities with respect to the guidelines and procedures described in the plan.

The Finance and Administration Officer, the Compliance Manager and the Science Manager have a responsibility, as custodians of the data and other information assets that support the business activities performed under their supervision, to ensure that those assets are adequately secured. They must also ensure that the appropriate information security guidelines, procedures and mechanisms described in the Plan are observed in the performance of these activities.

All personnel, whether employees, contractors, consultants or visitors, are required to comply with the information security guidelines, procedures and mechanisms and to play

an active role in protecting the information assets of the Commission. They must not access or operate these assets without authority and must report security breaches or exposures coming to their attention to the Executive Director.

Until the recruitment of an Information and Communications (ICT) Manager, The Executive Director is responsible for the day-to-day administration of the information security procedures and practices. On recruitment, the ICT Manager will assume responsibility for the day-to-day oversight of the Policy and associated Plan. He/she will report direct to the Executive Director on the performance of the information security procedures and practices.

Carelessness, negligence, deliberate breach of, or circumvention of, the principles of this Policy or associated Plan will lead to the appropriate disciplinary action as provided for in the Commission's Staff Regulations.

6. APPROACH

The Secretariat adopts a proactive approach to information security management and uses the standards on information security management **(ISO17799)** and risk management **(ISO17799/BS7799)** as the framework.

The Secretariat maintains a subscription to web-based ISO17799 resources.

Applying risk management techniques, information assets shall be periodically evaluated for the purpose of determining their individual value to the Commission and for the selection of appropriate protection measures.

Information processing facilities within the Secretariat's office premises will be risk assessed and appropriate security arrangements implemented. Access to processing facilities for confidential and sensitive information will be restricted to authorized personnel. Work place guidelines and procedures will describe accepted behavior within secure work areas. Security screening will be completed for all potential staff and service providers prior to recruitment. The employment contracts of all WCPFC staff and contracts with service providers will include detailed confidentiality agreements that reflect the obligation of full compliance with this Policy and associated plan.

7. PRINCIPLES

7.1 Obligations - Controls in place shall be effective as measured against security standards and compliance requirements that are of particular relevance to the Commission. These controls shall focus on the requirements outlined herein.

7.2 Authenticity - Users of information assets shall be uniquely identified.

7.3 Integrity - There shall be adequate protective controls and safeguards to ensure completeness and accuracy during the capture, storage, processing and presentation of information.

7.4 Confidentiality - There shall be adequate protective controls and safeguards to ensure that information is disclosed only to authorized users. Risks associated with third party access will be identified, types of access for authorized users adopted and protective controls described and implemented. Formal contracts for third party access to the Secretariat's information describe security compliance requirements provided for in the Policy.

7.5 Availability - There shall be adequate protective controls and safeguards to ensure that information can be delivered to the Secretariat's activities when required.

7.6 Reliability - There shall be adequate protective controls and safeguards to ensure that information available is complete and accurate.

7.7 Accountability - There shall be adequate protective controls and safeguards to ensure that responsibility for information undertaken by providers and users of information.

7.8 Conduct - Information assets owned, leased or rented by the Secretariat shall be solely for the conduct of Commission business. No private use, or use for any other purpose shall be permitted.

7.9 Education, Training and Awareness - The Secretariat recognizes the importance of security awareness raising, education and the need for training and continuing education programs for all Secretariat personnel and business partners such as service providers. Processes will be established to ensure corporate responsiveness to security incidents is builds on experience and lessons. Resources to address these requirements will be incorporated into the annual work program and budget considered by the Commission.

8. MONITORING AND REVIEW

Compliance with the Policy will be monitored on a regular basis. Security logs and audit trails will be produced to monitor the activities of users in their usage of information assets.

This Policy, with its supporting Plan, will be internally reviewed in October of each year to ensure completeness, effectiveness and usability. At 18 month intervals the Policy and the Plan will be reviewed by appropriately qualified and experienced experts recruited by international tender. Any proposed revisions to this Policy and Plan arising from reviews will be reported to the next regular session of the Commission for a decision on adoption, resource allocation and implementation.

(Signed)
Executive Director
(Dated)

Appendix A – Draft Framework for WCPFC Information Security Plan

The Information Security Policy will be complemented by a variety of other documents describing policies, procedures, guidelines and controls with regard to specific aspects of information security management in the Commission. These constitute an Information Security Plan which commits the management and staff of the WCPFC Secretariat to best practice for information security management. A draft framework for the known and anticipated elements of the Plan is presented below. This will be refined and elaborated upon as the operations of the Commission gradually increase.

1.0 Information Asset Identification and Inventory

Date:
Information Asset Name/Title
• Unique Identifier and Name Given to the Information Asset.

Information Contact(s)
• Name of person(s) knowledgeable about, or the custodian of, the Information Asset.
Name
Title
Address
Phone

Assignment of Security Responsibility
• Name of person responsible for security of the Information Asset.
Name
Title
Address
Phone

2.0 Overview of the Information Asset

General Description/Purpose/Classification Guidelines
Describe:
- Function or purpose of the information asset;
- Flow of the information from input to output;
- User organisations (internal and external) and type of data and processing provided;
- If applicable, the hardware/software configuration required for the information asset;
- If applicable, the interrelationship of this information asset to other information assets.

Information Security Requirements
Describe:
- Information security requirements in terms of the three basic protection requirements (confidentiality, integrity, and availability).

- For each of the three categories, indicate if the requirement is: Very High, High, Moderate, or Low;
- Any laws or regulations that specifically affect the confidentiality, integrity, availability, accountability, authenticity, and reliability of the information asset.

3.0 Risk Assessment Overview

Risk Assessment Methodology

Describe:

- Risk assessment methodology to identify the threats and vulnerabilities of the system;
- Date the review was conducted.
- If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment.

Review of Security Controls

List any independent security reviews conducted on the information asset in the last three years.

Threats and Vulnerabilities

Summarize the threats and vulnerabilities identified and the consequences arising from these.

Value of Assets

Summarize the value of the asset or the component of the asset, if applicable, and the basis for the valuation.

Level of Protection Required

- Briefly state the level of protection required including a Protection Profile if security products or system evaluation is required;
- Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system.

Acceptable Level of Risk

Briefly state the assessment of the residual risks accepted after implementing the controls identified.

Risk Treatment

Provide a high level matrix of the controls mapped to the threats identified.

4.0 Controls

4.1 Security policy

- Information Security Policy
- Review and evaluation of policy

4.2 Organizational security

- Information Security Infrastructure
- Security of Third Party Access
- Outsourcing

4.3 Asset classification and control

- Asset inventory
- Information classification guidelines

4.4 Personnel security

- Personnel Practices
- Security Awareness, Education and Training
- Incident Handling (Annex A)
- Disciplinary Process

4.5 Physical and environmental security

- Disposal and Re-use or equipment and software
- Secure Areas
- Equipment Security
- Clear Desk and Screen Policy
- Securing Unattended User Hardware
- Authorized Removal of Property

4.6 Communications and operations management

- Information and Software Exchange (Inter-agency) Agreements
- Email Policy
- Release of Public Information Policy – authorization and security
- Documented Operating Procedures
- Documented Operating Systems Security
- Network Management
- Management of removable media
- Configuration and Change Management
- Incident Management
- Segregation of Development and Operational Environments
- Capacity Planning
- System Acceptance
- Back-up of Information
- Logging Events and Faults
- Software and Information Exchange
- Protection Against Malicious Code

- Electronic Commerce Security
- Security of Electronic Mail
- Security of Electronic Office Systems
- Security of Electronically Published Information
- Media Handling and Security
- Operational Change Control

4.7 Access control

- User Identification and Authentication
- Access Control Policy
- User Access Management
- Review of Access Rights
- Network Access Controls
- Operating System Access Control
- Application Access Control
- Monitoring System Access and Use
- Authorization Process for Information Processing Facilities Mobile Computing
- Off-premises equipment and software security and protection
- media-in-transit
- Teleworking

4.8 Systems development and maintenance

- Specification of Security Requirements
- Application Controls
- Cryptography
- Restrictions to Software Package Modifications

4.9 Business continuity management

- Continuity impact analysis
- Continuity plans

4.10 Compliance

- Compliance with Legal and Regulatory Requirements
- Compliance with Security Policies and Standards
- System Audits

Annex A of Attachment A – WCPFC Security Incidents Management

Standard Classification of Security Incidents

Security incidents are to be classified according to:
- The type of incident, there are 8 accepted categories of these;
- The status of the incident when it is reported
- The causes of the incident.

Types of Security Incident

Access to data or a system without authorization
Such attempts may include:
- unauthorized use of an account (privileged or otherwise);
- unauthorized access to directories, files or media;
- placement of 'sniffing' hardware or software on network segment to capture data traveling across it;
- abuse of trust relationships (e.g, inter-domain trust) to access data.

Modification of data without authorization
Such attempts may include:
- placement of files:
  - new data;
  - trojan horse or virus code.
- deletion of data
- modification of data:
  - change of file permissions;
  - web page defacement;
  - alteration of file content.

Denial of service or disruption to system activity
Such incidents include:
- distributed denial of service attack (DDoS) causing loss of external network connections through packet flooding;
- exploitation of vulnerabilities causing network outage;
- causing system to crash;
- causing system to lose connectivity;
- causing system to partially or completely fail;
- physical loss or damage to systems.

Changes to system software/firmware, hardware or environment without approval
Such incidents include:
- installation of back door code without authorization (including violations by
- system developers);
- modification of system code without authorization;
- modification to cabling (patching, rack connections etc.);

- addition of software/hardware with malicious intent (e.g., keystroke logging or backdoor);
- unauthorized removal, addition or replacement of equipment.

Use of systems for processing or storage of data without authorization
Such incidents include:
- use of systems to perform unauthorized work;
- use of systems to perpetrate attacks on third parties (e.g. denial of service);
- use of systems to store unauthorized data (e.g. private files, sound or movie files, illegal copies of software).

Probe
Attempts to gain information that may be used to perpetrate an attack, including:
- automated scans;
- ping/port scan;
- trace route;
- targeted scans across whole, or large part of, IP range;
- social engineering;
- unexpected inquiries into network capabilities/vulnerabilities;
- unauthorized password resets.

Physical damage or loss rendering systems or data unavailable due to:
- theft;
- vandalism;
- fire;
- flood;
- damage.

Violation of an implicit or explicit security policy
As identified by the agency relative to its own security policies or procedures.

Status of the Incident
Incidents should be classified as:
- ongoing/continuing in real time;
- suspected;
- unsuccessful;
- successful;

They should then be identified as:
- accidental;
- deliberate.

Causes of the Incident
Incidents may be caused by:
- employees;
  - permanent;
  - casual/contractor;

- outside entity;
- natural disaster.

Liaison

In addition to reporting of the incident within the Secretariat, reporting to appropriate law enforcement authorities, regulatory bodies, information service providers and telecommunication operators is taken in a timely manner.

Appendix B - Glossary of Relevant Information Security Terms

To be completed.

Appendix C – Confidentiality of information during Secretariat service

This document sets out the Secretariat's confidentiality policy on information to which Staff may have access to during the course of their official duties with the WCPFC Secretariat. The policy is fully consistent with Staff Regulation 6 and all Secretariat Staff are required to expressly acknowledge it as well as its attached covenants.

BACKGROUND

All Staff, including work experience personnel, should be aware that confidentiality is an important aspect of the WCPFC Secretariat's work. This results from the organization's uniqueness and international character. It is dealt with specifically in WCPFC Staff Regulation 6.

All information obtained from the Secretariat work place, from WCPFC as a whole, from its Members, Participating Territories, Cooperating Non-Members (CCMs) and from associated third parties should be kept in confidence unless ruled otherwise. All Staff are thus bound by the implied and express confidentiality obligations and ethical considerations attached to these considerations. During their work in the Secretariat, Staff will learn much about WCPFC's business and that of its CCMs. Some of this information will be of a financial or legal nature, or may have a high degree of industrial confidentiality attached. The divulging of such information outside the Secretariat, will only be permissible on a direct order from, or through direct agreement with, the Commission or Executive Director. Failure to abide by these conditions, not only constitutes a violation of the Staff Member's Contract provisions, or work experience conditions, expressly dealing with confidentiality, it is also a breach of business ethics

If Staff are aware that they have disclosed any information arising from their work in the Secretariat to a third party, they should immediately notify their supervisor and the Executive Director.

Care is to be taken to ensure that Secretariat files or documents are not inadvertently provided to a third party in the absence of direction from the Executive Director. Equally, every effort should be made to ensure that other means of communication (i.e. telephone, email or any other form) are secure and will not expose the Secretariat to any accusation of improper behavior. Confidential papers should not be left exposed, particularly in easily accessible areas where others may see them.

Any discussions between Staff should be discreet. If there are any doubts about whether ancillary information should be divulged, the Staff Member responsible for such information should be consulted. All access to, or use of, data held by WCPFC should be in strict accordance with WCPFC's Information Security Policy and associated Plan provided to each staff member on their first day of duty with the Secretariat Other information (e.g. personnel details) should be treated in strict confidence.

WCPFC CONFIDENTIALTY POLICY

INTRODUCTION

Under the WCPFC Staff Contract and Staff Regulations, Secretariat staff are expected to perform certain duties during employment. The covenants attached to these duties include, *inter alia*, faithful service, attendance, lawful termination, discreteness and confidentiality, disclosure of possibly adverse personal information, disclosure of any misconduct by others and/or the Staff member concerned, obedience to lawful instructions, acting in WCPFC's best interests, and care and skill in the workplace. On cessation of employment (for whatever reason), the obligation duty not to disclose confidential information is most relevant. All Staff, including those on attachment or gaining work place experience, will expressly acknowledge this policy and attached covenants set out below.

COVENANTS ON WCPFC CONFIDENTIALITY

Staff shall:
(a) Not disclose or misuse confidential information that belongs to, or is held by, the WCPFC Secretariat, Commission or its Members, Participating Territories or Cooperating Non-Members when such information is obtained by the Staff Member during the course of his/her employment or work experience in the Secretariat.
(b) Not divulge at any time or for any reason, either during the continuance of his/her employment or work experience, or for a period of two years after termination of his/her employment, any of the affairs or secrets of the WCPFC Secretariat's or the Commission's business to any third party, person or persons without previous consent in writing from the Executive Director and/or Commission, nor shall he/she use or attempt to use any information which he/she may acquire in the course of his/her employment in any manner which may injure, or cause loss, or be calculated to injure or cause loss to the Secretariat and/or Commission.

SCHEDULE

I [Full Name] have read and understood the covenants set out above and sign in acknowledgement, thereof:

Period:

Staff Member's Signature:

Witness:

Date:

Appendix D – DRAFT Information classification guidelines

This document sets out the Secretariat's draft information security classification guidelines. Each information type will be given two security classifications:

- A confidentiality classification – this classification reflects the damage that would be done to the operations or credibility of the Commission as a consequence of the unauthorized disclosure of such information;
- A continuity classification - this classification reflects the damage that would be done to the operations of the Commission as a consequence of short or long term loss (or extensive damage to) such information.

The security controls implemented by the Commission will reflect the classifications given to each information type.

Information type	Confidentiality classification	Continuity classification
Operational level Catch Effort data	Medium	High
Operational level Observer Catch Effort data	Medium	High
Records of vessel unloading	Medium	High
Biological data	Low	High
Tagging data	Low	High
Vessel and gear attributes	Low	Medium
Oceanographic and meteorological data	Public	Medium
Authorization to fish	Public	Medium
Transhipment	High	Medium
VMS Register/Vessel Record	Public	Medium
VMS Vessel position, direction and speed	High	High
Boarding and Inspection	High	High
Certified observer personnel	Low	Low
Certified inspection personnel	Low	Low
Catch documentation scheme	High	High
Port State measures and procedures	Public	Low
Violations and infringements	High	High