INFORMATION SECURITY POLICY

Priorities

As adopted by the Third Regular Session of the Commisison
11-15 December 2007
Apia, Samoa

Introduction

This “Priorities” document is intended for a small, evolving, Commission. It establishes a management framework to initiate and control the implementation of information security within the WCPFC. It consists of the principle elements of the more extensive Policy, based on ISO17799, and presented in Part 1.

The complete ISP is intended for large organizations and is based on the level of detail in ISO17799. Most of what is in this document is common sense. Much of its implementation can be achieved through behavioral adaptation by personnel associated with WCPFC information rather than through a significant investment in assets and technologies.

There is no intention that the ISP will be implemented in full in its first year of operation. Rather it will be phased in over 5-10 years as the organisation evolves. Implementation will be subject to the priority the WCPFC members place on information security and the resources they are willing to commit to its management. Those activities and tasks that are of short, medium and longer term nature have been identified. A document with the full ISO17799 is also available *[reference: WCPFC ISP Part 2 Version 3, 1 July 2007]*.

TABLE OF CONTENTS

Page

1. ORGANIZATION OF INFORMATION SECURITY 5

1.1 INTERNAL ORGANIZATION 5
1.1.1 WCPFC commitment to information security 5
1.1.2 Information security co-ordination 5
1.1.3 Allocation of information security responsibilities 6
1.1.4 Confidentiality agreements 6

2. ASSET MANAGEMENT 8

2.1 RESPONSIBILITY FOR ASSETS 8
2.2 INFORMATION CLASSIFICATION 8

3. HUMAN RESOURCES SECURITY 9

3.1 PRIOR TO EMPLOYMENT 9
3.2 DURING EMPLOYMENT 9
3.3 TERMINATION OR CHANGE OF EMPLOYMENT 9

4. PHYSICAL AND ENVIRONMENTAL SECURITY 10

4.1 SECURE AREAS 10

5. COMMUNICATIONS AND OPERATIONS MANAGEMENT 11

5.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES 11
5.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT 11
5.3 PROTECTION AGAINST MALICIOUS CODE 11
5.4 BACK-UP 12
5.5 MEDIA HANDLING 12
5.6 EXCHANGE OF INFORMATION 12
5.7 MONITORING 12
5.7.1 Fault logging 12

6. ACCESS CONTROL 13

6.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL 13
6.2 USER ACCESS MANAGEMENT 13
6.2.1 Privilege management 13
6.2.2 User password management 13
6.3 USER RESPONSIBILITIES 14
6.3.1 Password use 14
6.3.2 Unattended user equipment 15
6.4 OPERATING SYSTEM ACCESS CONTROL 15
6.4.1 User identification and authentication 15
6.5 MOBILE COMPUTING AND TELEWORKING 15

7. ACQUISITION AND MAINTENANCE 16

7.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS 16
7.2 CORRECT PROCESSING IN APPLICATIONS 16

8. INFORMATION SECURITY INCIDENT MANAGEMENT 17

8.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES 17
8.1.1 Reporting security weaknesses 17
8.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS 17

9. BUSINESS CONTINUITY MANAGEMENT 18

9.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT 18

10. COMPLIANCE 19

10.1 COMPLIANCE WITH LEGAL REQUIREMENTS 19
10.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS 19
10.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS 19

Organization of information security

This chapter deals with the organization and management of information security both within the WCPFC (including, to the extent practical, Commission Members, Participating Territories, and Cooperating Non-members) and external to the WCPFC.

Internal organization

This section establishes a management framework to initiate and control the implementation of information security within the WCPFC. Consistent with, and complementary to, the information management policies and procedures adopted by the Commission, the Executive Director approves the Information Security Policy (ISP), assigns security roles and co-ordinates/ reviews the implementation of security across the WCPFC. Contacts with external security specialists or groups, including relevant authorities, will be developed to keep up with industry trends, monitor standards and assessment methods and provide suitable liaison points when handling information security incidents.

WCPFC commitment to information security

The WCPFC actively supports security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

WCPFC Secretariat is responsible for:

a. ensuring that information security goals are identified, meet the WCPFC requirements, and are integrated in relevant processes;

b. formulating, reviewing, and approving information security policy;

c. reviewing the effectiveness of the implementation of the information security policy;

d. providing clear direction and visible management support for security initiatives;

e. providing the resources needed for information security;

f. approving assignment of specific roles and responsibilities for information security across the WCPFC;

g. initiating plans and programs to maintain information security awareness; and

h. ensuring that the implementation of information security controls is coordinated across the WCPFC.

Information security co-ordination

Information security co-ordination involves the co-operation and collaboration of managers, users, administrators, application designers, auditors and security personnel, and specialists. This activity includes:

a. ensuring that security activities are executed in compliance with the information security policy;

b. identifying how to handle non-compliances;

c. approving methodologies and processes for information security, e.g. risk assessment and information classification;

d. identifying significant threat changes and exposure of information and information processing facilities to threats;

e. assessing the adequacy and coordinating the implementation of information security controls;

f. effectively promoting information security education, training and awareness throughout the WCPFC; and

g. evaluating information received from the monitoring and reviewing of information security incidents, and recommend appropriate actions in response to identified information security incidents.

Allocation of information security responsibilities

The allocation of information security responsibilities is done in accordance with the ISP. Responsibilities for the protection of individual assets and for carrying out specific security processes are identified. Areas for which individuals are responsible are clearly stated; in particular the following takes place:

a. the assets and security processes associated with computers and networks within the WCPFC are identified and clearly defined;

b. the entity responsible for each asset or security process is assigned and the details of this responsibility are documented; and

c. authorization levels are clearly defined and documented.

Confidentiality agreements

Confidentiality and non-disclosure agreements protect organisational information and inform signatories of their responsibility to protect, use, and disclose information in a responsible and authorised manner. Requirements for confidentiality or non-disclosure agreements reflecting the WCPFC's needs for the protection of information have been identified and are regularly reviewed. The WCPFC's non-disclosure agreements address the requirement to protect the confidentiality of information using legally enforceable terms. To identify requirements for the non-disclosure agreements, the following elements were considered:

a. a definition of the information to be protected (e.g. confidential information);

b. expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;

c. required actions when an agreement is terminated;

d. responsibilities and actions of signatories to avoid unauthorized information disclosure (such as ‘need to know’);

e. ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;

f. the permitted use of confidential information, and rights of the signatory to use information;

g. the right to audit and monitor activities that involve confidential information;

h. process for notification and reporting of unauthorized disclosure or confidential information breaches;

i. terms for information to be returned or destroyed at agreement cessation; and

j. expected actions to be taken in case of a breach of this agreement.

Asset management

The objective of this chapter is to ensure that all assets are accounted for and have a nominated owner.

Responsibility for assets

Owners will be identified for all assets and the responsibility for the maintenance of appropriate controls will be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.

Information classification

Information will be classified in terms of its value, legal requirements, sensitivity, and criticality to the WCPFC. Classifications and associated protective controls for information will take account of business needs for sharing or restricting information and the business impacts associated with such needs. Classification guidelines include conventions for initial classification and reclassification over time; in accordance with some predetermined access control policy. It is the responsibility of the asset owner to define the classification of an asset, periodically review it, and ensure it is kept up to date and at the appropriate level.

Human resources security

This chapter will ensure that users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of WCPFC facilities and assets.

Prior to employment

The security responsibilities will be addressed prior to employment in adequate job descriptions and in terms and conditions of employment. All candidates for users will be screened. Users of information processing facilities will sign an agreement on their security roles and responsibilities.

During employment

Management responsibilities will be defined to ensure that security is applied throughout an individual's employment within the WCPFC. An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities will be provided to all users to minimize possible security risks. A formal disciplinary process for handling security breaches will be established.

Termination or change of employment

Responsibilities will be in place to ensure a user's exit from the WCPFC is managed, and that the return of all equipment and the removal of all access rights are completed. Change of responsibilities and employments within the WCPFC will be managed as the termination of the respective responsibility or employment in line with this section, and any new employments will be managed as described in section 3.1.

Physical and environmental security

Secure areas

Critical or sensitive information processing facilities will be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They will be physically protected from unauthorized access, damage, and interference. The protection provided will be commensurate with the identified risks.

Communications and operations management

Operational procedures and responsibilities

Responsibilities and procedures for the management and operation of all information processing facilities will be established. This is to ensure the correct and secure operation of these facilities.

Third party service delivery management

The WCPFC will check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party.

Protection against malicious code

Precautions are required to prevent and detect the introduction of malicious code. Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users will be made aware of the dangers of malicious code.

Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures will be implemented. Protection against malicious code will be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls. The following will be implemented:

a. establishing a formal policy prohibiting the use of unauthorized software;

b. installation and regular update of malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the checks carried out will include:

    i. checking any files on electronic or optical media, and files received over networks, for malicious code before use;

    ii. checking electronic mail attachments and downloads for malicious code before use; this check will be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the WCPFC; and

    iii. checking web pages for malicious code;

Back-up

Routine procedures will be established to implement the agreed back-up policy and strategy for taking back-up copies of data and rehearsing their timely restoration.

Media handling

Media will be controlled and physically protected. Appropriate operating procedures will be established to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.

Exchange of information

Exchanges of information and software between organizations will be based on a formal exchange policy, carried out in line with exchange agreements, and will be compliant with any relevant legislation. Procedures and standards will be established to protect information and physical media containing information in transit.

Monitoring

Systems will be monitored and information security events will be recorded. Operator logs and fault logging will be used to ensure information system problems are identified. WCPFC will comply with all relevant legal requirements applicable to its monitoring and logging activities. System monitoring will be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

Fault logging

Faults reported by users or by system programs related to problems with information processing or communications systems will be logged. There will be clear rules for handling reported faults including:

a. review of fault logs to ensure that faults have been satisfactorily resolved; and

b. review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized.

Access control

Business requirement for access control

Access to information, information processing facilities, and business processes will be controlled on the basis of business and security requirements. Access control rules will take account of policies for information dissemination and authorization.

User access management

Procedures will be in place to control the allocation of access rights to information systems and services. The procedures will cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.

Privilege management

The allocation and use of privileges will be restricted and controlled. Multi-user systems that require protection against unauthorized access will have the allocation of privileges controlled through a formal authorization process. The following steps will be implemented:

a. the access privileges associated with each computer system will be identified;

b. privileges will be allocated to users on a need-to-use basis in line with the access control policy i.e. the minimum requirement for their functional role only when needed; and

c. an authorization process and a record of all privileges allocated will be maintained. Privileges will not be granted until the authorization process is complete.

User password management

The allocation of passwords will be controlled through a formal management process. The process will include the following requirements:

a. users will be required to sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group; this signed statement could be included in the terms and conditions of employment;

b. when users are required to maintain their own passwords they will be provided initially with a secure temporary password, which they are forced to change immediately;

c. establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password;

d. temporary passwords will be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages will be avoided;

e. temporary passwords will be unique to an individual and will not be guessable;

f. users will acknowledge receipt of passwords;

g. passwords will never be stored on computer systems in an unprotected form; and

h. default vendor passwords will be altered following installation of systems or software.

User responsibilities

The co-operation of authorized users is essential for effective security. Users will be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment. A clear desk and clear screen policy will be implemented to reduce the risk of unauthorized access or damage to papers, media, and information processing facilities.

Password use

Users will be required to follow good security practices in the selection and use of passwords. All users will be advised to:

a. keep passwords confidential;

b. avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved;

c. change passwords whenever there is any indication of possible system or password compromise;

d. select quality passwords with sufficient minimum length which are:

    i. easy to remember;

    ii. not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;

    iii. not vulnerable to dictionary attacks (do not consist of words included in dictionaries);

    iv. free of consecutive identical, all-numeric or all-alphabetic characters;

e. change passwords at regular intervals (passwords for privileged accounts will be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;

f. change temporary passwords at the first log-on;

g. not include passwords in any automated log-on process, e.g. stored in a macro or function key;

h. not share individual user passwords; and

i. not use the same password for business and non-business purposes.

Unattended user equipment

Users will ensure that unattended equipment has appropriate protection. All users will be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.

Operating system access control

Security facilities will be used to restrict access to operating systems to authorized users. The facilities will be capable of the following:

a. authenticating authorized users, in accordance with a defined access control policy;

b. recording successful and failed system authentication attempts;

c. recording the use of special system privileges;

d. issuing alarms when system security policies are breached;

e. providing appropriate means for authentication; and

f. where appropriate, restricting the connection time of users.

User identification and authentication

All users will have a unique identifier (user ID) for their personal use only, and a suitable authentication technique will be chosen to substantiate the claimed identity of a user. This control will be applied for all types of users. User IDs will be used to trace activities to the responsible individual. Regular user activities will not be performed from privileged accounts.

Mobile computing and teleworking

To ensure information security when using mobile computing and teleworking facilities, the protection required will be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment will be considered and appropriate protection applied. In the case of teleworking the WCPFC will apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.

Acquisition and maintenance

Security requirements of information systems

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements will be identified and agreed prior to the development and/or implementation of information systems. All security requirements will be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

Correct processing in applications

Appropriate controls will be designed into applications, including user developed applications to ensure correct processing. These controls will include the validation of input data, internal processing and output data. Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls will be determined on the basis of security requirements and risk assessment.

Information security incident management

Reporting information security events and weaknesses

Formal event reporting and escalation procedures will be in place. All users will be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of WCPFC assets. They will be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

Reporting security weaknesses

All users of information systems and services will be required to note and report any observed or suspected security weaknesses in systems or services. All users will report these matters either to their management or directly to their service provider as quickly as possible in order to prevent information security incidents. The reporting mechanism will be as easy, accessible, and available as possible. They will be informed that they will not, in any circumstances, attempt to prove a suspected weakness.

Management of information security incidents and improvements

Responsibilities and procedures will be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement will be applied to the response to, monitoring, evaluating, and overall management of information security incidents. Where evidence is required, it will be collected to ensure compliance with legal requirements.

Business continuity management

Information security aspects of business continuity management

A business continuity management process will be implemented to minimize the impact on the WCPFC and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process will identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

Compliance

Compliance with legal requirements

The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements. Advice on specific legal requirements will be sought from the WCPFC's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow).

Compliance with security policies and standards

The security of information systems will be regularly reviewed. Such reviews will be performed against the appropriate security policies and the technical platforms and information systems will be audited for compliance with applicable security implementation standards and documented security controls.

Information systems audit considerations

There will be controls to safeguard operational systems and audit tools during information systems audits. Protection is also required to safeguard the integrity and prevent misuse of audit tools.

WESTERN AND CENTRAL PACIFIC FISHERIES COMMISSION

(WCPFC)

INFORMATION SECURITY POLICY

Part 1

1 July 2007

CHANGE CONTROL RECORD

VERSION	DATE	DESCRIPTION OF CHANGES	AFFECTED PAGES
1.0	July 2006	Initial Draft	All
1.1	17 June 2007	Updated Draft	All
2	1 July 2007	Second Draft	All

TABLE OF CONTENTS

Page

1. INTRODUCTION 23

1.1 PURPOSE 23
1.2 CONTEXT 23
1.3 GOALS AND OBJECTIVES 23
1.4 SCOPE 24
1.5 CATEGORIZATION OF INFORMATION ASSETS 25
1.6 RESPONSIBILITIES 25
1.6.1 Executive Director 25
1.6.2 Finance / Administration Officer, Compliance and Science Manager 26
1.6.3 Other Personnel 26
1.7 APPROACH 26
1.8 PRINCIPLES 27
1.9 MONITORING AND REVIEW 27

APPENDIX A – DRAFT FRAMEWORK FOR WCPFC INFORMATION SECURITY PLAN 29

1.0 INFORMATION ASSET IDENTIFICATION AND INVENTORY 29
2.0 OVERVIEW OF THE INFORMATION ASSET 29
3.0 RISK ASSESSMENT OVERVIEW 30

APPENDIX B – GLOSSARY OF RELEVANT INFORMATION SECURITY TERMS 32

APPENDIX C – INFORMATION SECURITY CLASSIFICATION GUIDELINES 36

Introduction

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 that is either commercially, personally or politically sensitive it manages on behalf of Members, Cooperating Non-members and Participating Territories (CCMs), 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, CCMs. 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. Based on the policies and procedures for information management adopted by the Commission, this Policy sets a clear direction, and demonstrates support for, and commitment to the management of information security in respect of all the Commission's business relationships. It is complemented by an Information Security Plan which is elaborated in a companion document (Part 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.

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 Commission CCMs and other stakeholders in the WCPFC;
- Minimise the possibility of a threat to information security causing loss or damage to the WCPFC Secretariat, its CCMs 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, CCMs 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.

SCOPE

This Policy applies to:

- All users of WCPFC Secretariat information including service providers to the Secretariat[1];
- 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;

[1] The Policy applies to the Secretariat only. To the extent practical, the Commission encourages CCMs to develop and implement information security policies and procedures that are consistent with the Commission Secretariat's ISP in respect of WCPFC-related information and data.

- 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 include:

- Technical reports, systems documentation, user manuals, continuity plans, contracts, guidelines and procedures.

Personnel include:

- Employees, contractors, consultants, service providers, representatives of Commission Members, Participating Territories, Cooperating Non-members (CCMs) and other stakeholders that access the Secretariat's information and data.

Categorization of Information Assets

The information owner must identify the sensitivity of information for which they are responsible when the unauthorized disclosure of the information could reasonably be expected to cause injury to, or impact of WCPFC interests. Information that is considered sensitive must be categorized and marked based on the degree of potential injury or impact (low, medium, or high).

Members must identify and categorize assets, especially critical services, based on the degree of injury (low, medium, high) that could reasonably be expected to result from compromise to their availability or integrity. They must consider the value of assets in determining injury.

The WCPFC members must limit access to sensitive information to those individuals who have a need to know the information.

RESPONSIBILITIES

Executive Director

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.

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.

Finance / Administration Officer, Compliance and Science Manager

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.

Other Personnel

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.

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.

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.

PRINCIPLES

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.

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

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

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.

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

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

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

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.

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.

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 March 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.

Appendix B – Glossary of Relevant Information Security Terms

Acceptable Level of Risk - A judicious and carefully considered assessment that an information technology (IT) activity or network meets the minimum requirements of applicable security directives.

Access rights – The permission to use information or a system. Access rights are usually denoted as Read, Write, and Delete.

Accountability - The property that ensures that the actions of an entity may be traced uniquely to that entity.

Administrative Security - The management constraints; operational, administrative, and accountability procedures and supplemental controls established to provide an acceptable level of protection for information and assets.

Asset - A component or part of the total system or network to which the organization directly assigns a value to represent the level of importance to the "business" or operations/operational mission of the organization, and therefore warrants an appropriate level of protection. Assets types include: information, hardware, communications equipment, firmware, documents/publications, environmental equipment, people/staff, infrastructure, goodwill, money, income, organizational integrity, customer confidence, services and organizational image.

Assurance - The degree of confidence that the implemented security functions of an IT system or product adequately enforce the system security policy. Alternatively, the degree of confidence that the implemented system meets its stated security requirements.

Attack - The act of aggressively trying to bypass security controls on an IT system or network. The fact that the attack is made does not mean it will succeed. The success depends on the vulnerability of the system, network or activity and the effectiveness of the safeguards in place.

Authentication - The act of verifying the claimed identity of an entity.

Authorization levels - The granting of rights, which includes the granting of access based on access rights.

Availability - The accessibility of systems, programs, services and information to authorized users when needed and without undue delay.

Breach of Security - When any sensitive information and/or assets have been compromised. Without restricting its scope, a breach may include compromise in circumstances that make it probable that a breach has occurred.

Capability – A measure of a threat agent's ability (including the level of effort required) to successfully attack an asset by exploiting its vulnerabilities.

Classification - A determination that information requires a specific degree of protection against unauthorized disclosure together with a designation signifying that such a determination has been made.

Compromise - A violation of the security policy of a system or network such that an unauthorized disclosure, modification, removal, interruption or destruction of sensitive information may have occurred.

Confidentiality - The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Configuration Management - The management of changes made to a system's hardware, software, and firmware and to the documentation that chronicles changes to the equipment, personnel and security systems throughout the development and operational life of the system.

Continuity of Operations - The maintenance of essential services for an information system after a major failure. The failure may result from natural causes (such as fire, flood or earthquakes) or from deliberate events (such as sabotage).

Data Integrity - The property that data is being handled as intended and has not been exposed to accidental or intentional modification or destruction.

Denial of Service - The prevention or delay of legitimate or authorized access, or the unauthorized withholding of critical information or resources.

Disclosure - A violation of the security policy of a system in which information has been made available to unauthorized entities.

Encryption - The transformation of readable data or information into an unreadable stream of alpha/numeric using a reversible coding process.

External Parties – This includes anyone not an official of a CCM.

Hacker(s) - All persons, criminal or otherwise, who penetrate computers or communications networks with malicious intent.

Identification - A unique, and perhaps auditable representation of each individual user within an IT system, usually in the form of a string of characters (e.g., LoginID).

Integrity - The accuracy and completeness of information and assets and the authenticity of transactions.

IT Security Policy - Rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization and its IT systems.

Loss - A quantitative measure of harm or deprivation resulting from a compromise.

Loss of Confidence - The condition of losing faith in the organization's information and/or IT systems.

Loss of Service - The condition of not being able to produce and/or deliver a specific service, or have a required service delayed to the point where it causes interference with normal day-to-day activities.

Managed Risk - Attained when the extent of security protection is commensurate with the cost of implementing security measures and the risk: the likelihood of a breakdown in security and the impact that it would have on a program.

Motivation - A measure combining the potential benefit to the threat agent, and the resources available to the threat agent.

Owner – The person or organization responsible for an asset including its proper protection.

Permissions - A description of the type of authorized interactions a subject can have with an object. Permissions include: read, write, execute, add, modify, and delete.

Personnel Security - The procedures established to ensure that all personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances.

Physical Security - The application of physical barriers and control procedures to provide protection, detection and response mechanisms used in the physical environment to control access to sensitive information and assets.

Procedural Security - Approved management constraints; operational, administrative, and accountability procedures; and other supplemental controls established to provide protection for sensitive information.

Reliability - The property of an IT system to maintain consistent, intended and trustworthy operation over a given period of time.

Risk - Intuitively, the adverse effects that can result if a vulnerability is exploited or if a threat is actualized. In some contexts, a risk is a measure of the likelihood of adverse effects or the product of the likelihood and the quantified consequences. There is no standard definition. (Based on Computer Related Risks)

Risk Management - The process by which resources are planned, organized, directed, and controlled to ensure the risk of operating a system remains within acceptable bounds at optimal cost.

Safeguard(s) - The approved minimum security measure(s) and controls which, when correctly employed, will prevent or reduce the risk of exploitation of specific vulnerability(ies) which would compromise an IT system.

Security Screening - The type of personnel background check that, with a need to know, is required for access to sensitive information and assets.

Security Officer - A person who is made responsible for the overall security of an IT system. (Note: The security officer will normally consider physical, personnel and procedural security.)

Security Requirement(s) - The specification of a security function(s) needed within an IT system, which if satisfied will result in the IT system meeting its Target Residual Risk.

Sensitive Information - Information that requires protection due to the risk of loss or harm that could result from inadvertent or deliberate disclosure, modification, or destruction.

Threat - Any potential event or act that could cause one or more of the following to occur: unauthorized disclosure, destruction, removal, modification or interruption of sensitive or critical information, assets or services. A threat can be natural, deliberate or accidental.

Vulnerability - A quantifiable, threat-independent characteristic or attribute of any asset within a system boundary or environment in which it operates and which increases the probability of a threat event occurring and causing harm in terms of confidentiality, availability and/or integrity, or increases the severity of the effects of a threat event if it occurs.

Appendix C – Information Security 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

INFORMATION SECURITY POLICY

Part 2
WCPFC Operational Security Standards

As adopted by the Third Regular Session of the Commisison
11-15 December 2007
Apia, Samoa

Introduction

This ISP is intended for large organisations and is based on the level of detail in ISO17799. Most of what is in this document is common sense. Much of its implementation can be achieved through behavioral adaptation by personnel associated with WCPFC information rather than a significant investment in assets and technologies. There is no intention that the ISP will be implemented in full in its first year of operation. This ISP will be phased in over 5-10 years as the organisation evolves. Implementation will be subject to the priority the WCPFC members place on information security and the resources they are willing to commit to its management. Those activities and tasks that are of short, medium and longer term nature have been identified. Due to the logistical and resource constraints to the Secretariat implementing an ISP as described, a document highlighting priority areas is also available *[reference: WCPFC ISP Priorities Version 2, 2 July 2007]*.

TABLE OF CONTENTS

Page

1. ORGANIZATION OF INFORMATION SECURITY 43

1.1 INTERNAL ORGANIZATION 43
1.1.1 WCPFC commitment to information security 43
1.1.2 Information security co-ordination 44
1.1.3 Allocation of information security responsibilities 44
1.1.4 Authorization process for information processing facilities 44
1.1.5 Confidentiality agreements 45
1.1.6 Contact with authorities 45
1.1.7 Contact with special interest groups with respect to information security 46
1.1.8 Independent review of information security 46
1.2 EXTERNAL PARTIES 46
1.2.1 Identification of risks related to external parties 46

2. ASSET MANAGEMENT 48

2.1 RESPONSIBILITY FOR ASSETS 48
2.1.1 Inventory of assets 48
2.1.2 Ownership of assets 48
2.1.3 Acceptable use of assets 49
2.2 INFORMATION CLASSIFICATION 49
2.2.1 Classification guidelines 49
2.2.2 Information labeling and handling 49

3. HUMAN RESOURCES SECURITY 50

3.1 PRIOR TO EMPLOYMENT 50
3.1.1 Roles and responsibilities 50
3.1.2 Screening 50
3.1.3 Terms and conditions of employment 51
3.2 DURING EMPLOYMENT 51
3.2.1 Management responsibilities 51
3.2.2 Information security awareness, education, and training 52
3.2.3 Disciplinary process 52
3.3 TERMINATION OR CHANGE OF EMPLOYMENT 53
3.3.1 Termination responsibilities 53
3.3.2 Return of assets 53
3.3.3 Removal of access rights 53

4. PHYSICAL AND ENVIRONMENTAL SECURITY 55

4.1 SECURE AREAS 55
4.1.1 Physical security perimeter 55
4.1.2 Physical entry controls 55
4.1.3 Securing offices, rooms, and facilities 56
4.1.4 Protecting against external and environmental threats 56
4.1.5 Working in secure areas 57
4.1.6 Public access, delivery, and loading areas 57
4.2 EQUIPMENT SECURITY 57
4.2.1 Equipment placement and protection 57
4.2.2 Supporting utilities 58
4.2.3 Cabling security 58
4.2.4 Equipment maintenance 59
4.2.5 Security of equipment off-premises 59
4.2.6 Secure disposal or re-use of equipment 59
4.2.7 Removal of property 60

5. COMMUNICATIONS AND OPERATIONS MANAGEMENT 61

5.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES 61
5.1.1 Documented operating procedures 61
5.1.2 Change management 61
5.1.3 Segregation of duties 62
5.1.4 Separation of development, test, and operational facilities 62
5.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT 63
5.2.1 Service delivery 63
5.2.2 Monitoring and review of third party services 63
5.2.3 Managing changes to third party services 63
5.3 SYSTEM PLANNING AND ACCEPTANCE 64
5.3.1 Capacity management 64
5.3.2 System acceptance 64
5.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE 65
5.4.1 Controls against malicious code 65
5.4.2 Controls against mobile code 66
5.5 BACK-UP 67
5.5.1 Information back-up 67
5.6 NETWORK SECURITY MANAGEMENT 67
5.6.1 Network controls 68
5.6.2 Security of network services 68
5.7 MEDIA HANDLING 68
5.7.1 Management of removable media 68
5.7.2 Disposal of media 69
5.7.3 Information handling procedures 69
5.7.4 Security of system documentation 69
5.8 EXCHANGE OF INFORMATION 70
5.8.1 Information exchange policies and procedures 70
5.8.2 Exchange agreements 71
5.8.3 Physical media in transit 72
5.8.4 Electronic messaging 72
5.8.5 Business information systems 73
5.9 ELECTRONIC COMMERCE SERVICES 73
5.9.1 Electronic commerce 73
5.9.2 On-Line Transactions 74
5.9.3 Publicly available information 75
5.10 MONITORING 75
5.10.1 Audit logging 75
5.10.2 Monitoring system use 76
5.10.3 Protection of log information 77
5.10.4 Administrator and operator logs 77
5.10.5 Fault logging 77
5.10.6 Clock synchronization 78

6. ACCESS CONTROL 79

6.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL 79
6.1.1 Access control policy 79
6.2 USER ACCESS MANAGEMENT 79
6.2.1 User registration 80
6.2.2 Privilege management 80
6.2.3 User password management 81
6.2.4 Review of user access rights 81
6.3 USER RESPONSIBILITIES 82
6.3.1 Password use 82
6.3.2 Unattended user equipment 82

6.3.3 Clear desk and clear screen policy *83*
6.4 NETWORK ACCESS CONTROL 83
6.4.1 Policy on use of network services *84*
6.4.2 User authentication for external connections *84*
6.4.3 Equipment identification in networks *84*
6.4.4 Remote diagnostic and configuration port protection *84*
6.4.5 Segregation in networks *85*
6.4.6 Network connection control *85*
6.4.7 Network routing control *85*
6.5 OPERATING SYSTEM ACCESS CONTROL 85
6.5.1 Secure log-on procedures *86*
6.5.2 User identification and authentication *87*
6.5.3 Password management system *87*
6.5.4 Use of system utilities *87*
6.5.5 Session time-out *88*
6.5.6 Limitation of connection time *88*
6.6 APPLICATION AND INFORMATION ACCESS CONTROL 88
6.6.1 Information access restriction *88*
6.6.2 Sensitive system isolation *89*
6.7 MOBILE COMPUTING AND TELEWORKING 89
6.7.1 Mobile computing and communications *89*
6.7.2 Teleworking *90*

7. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE 92

7.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS 92
7.1.1 Security requirements analysis and specification *92*
7.2 CORRECT PROCESSING IN APPLICATIONS 92
7.2.1 Input data validation *93*
7.2.2 Control of internal processing *93*
7.2.3 Message integrity *94*
7.2.4 Output data validation *94*
7.3 CRYPTOGRAPHIC CONTROLS 95
7.3.1 Policy on the use of cryptographic controls *95*
7.3.2 Key management *95*
7.4 SECURITY OF SYSTEM FILES 96
7.4.1 Control of operational software *96*
7.4.2 Protection of system test data *97*
7.4.3 Access control to program source code *98*
7.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES 98
7.5.1 Change control procedures *98*
7.5.2 Technical review of applications after operating system changes *99*
7.5.3 Restrictions on changes to software packages *100*
7.5.4 Information leakage *100*
7.5.5 Outsourced software development *100*
7.6 TECHNICAL VULNERABILITY MANAGEMENT 101
7.6.1 Control of technical vulnerabilities *101*

8. INFORMATION SECURITY INCIDENT MANAGEMENT 103

8.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES 103
8.1.1 Reporting information security events *103*
8.1.2 Reporting security weaknesses *104*
8.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS 104
8.2.1 Responsibilities and procedures *104*
8.2.2 Learning from information security incidents *105*
8.2.3 Collection of evidence *106*

9. BUSINESS CONTINUITY MANAGEMENT 107

9.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT 107
9.1.1 Including information security in the business continuity management process 107
9.1.2 Business continuity and risk assessment 108
9.1.3 Developing and implementing continuity plans including information security 108
9.1.4 Business continuity planning framework 108
9.1.5 Testing, maintaining and re-assessing business continuity plans 109

10. COMPLIANCE 110

10.1 COMPLIANCE WITH LEGAL REQUIREMENTS 110
10.1.1 Identification of applicable legislation 110
10.1.2 Intellectual property rights (IPR) 110
10.1.3 Protection of organizational records 111
10.1.4 Data protection and privacy of personal information 112
10.1.5 Prevention of misuse of information processing facilities 112
10.1.6 Regulation of cryptographic controls 112
10.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE 113
10.2.1 Compliance with security policies and standards 113
10.2.2 Technical compliance checking 113
10.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS 114
10.3.1 Information systems audit controls 114
10.3.2 Protection of information systems audit tools 114

Organization of information security

This chapter deals with the organization and management of information security both within the WCPFC (including, to the extent practical, Commission Members, Participating Territories, and Cooperating Non-members[2] (CCMs)) and external to the WCPFC.

Internal organization

This section establishes a management framework to initiate and control the implementation of information security within the WCPFC. Consistent with, and complementary to, the information management policies and procedures adopted by the Commission, the Executive Director approves the Information Security Policy (ISP), assigns security roles and co-ordinates/ reviews the implementation of security across the WCPFC. Contacts with external security specialists or groups, including relevant authorities, will be developed to keep up with industry trends, monitor standards and assessment methods and provide suitable liaison points when handling information security incidents.

WCPFC commitment to information security

The WCPFC actively supports security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

WCPFC Secretariat is responsible for:

i. ensuring that information security goals are identified, meet the Commission's requirements, and are integrated in relevant processes;

j. formulating, reviewing, and approving information security policy;

k. reviewing the effectiveness of the implementation of the information security policy;

l. providing clear direction and visible management support for security initiatives;

m. providing the resources needed for information security;

n. approving assignment of specific roles and responsibilities for information security, to the extent possible, across the WCPFC;

o. initiating plans and programs to maintain information security awareness; and

p. ensuring that, to the extent practical, the implementation of information security controls is coordinated across the WCPFC.

[Implementation – short term]

[2] The Policy applies to the Secretariat only. To the extent practical, the Commission encourages CCMs to develop and implement information security policies and procedures that are consistent with the Commission Secretariat's ISP in respect of WCPFC-related information and data.

Information security co-ordination

Information security co-ordination involves the co-operation and collaboration of managers, users, administrators, application designers, auditors and security personnel, and specialists. This activity includes:

h. ensuring that security activities are executed in compliance with the information security policy;

i. identifying how to handle non-compliances;

j. approving methodologies and processes for information security, e.g. risk assessment and information classification;

k. identifying significant threat changes and exposure of information and information processing facilities to threats;

l. assessing the adequacy and coordinating the implementation of information security controls;

m. effectively promoting information security education, training and awareness throughout the WCPFC Secretariat and among WCPFC stakeholders; and

n. evaluating information received from the monitoring and reviewing of information security incidents, and recommend appropriate actions in response to identified information security incidents.

[Implementation – short term]

Allocation of information security responsibilities

The allocation of information security responsibilities is done in accordance with the ISP. Responsibilities for the protection of individual assets and for carrying out specific security processes are identified. Areas for which individuals are responsible are clearly stated; in particular the following takes place:

d. the assets and security processes associated with computers and networks within the WCPFC are identified and clearly defined;

e. the entity responsible for each asset or security process is assigned and the details of this responsibility are documented; and

f. authorization levels are clearly defined and documented.

[Implementation – short term]

Authorization process for information processing facilities

New facilities need appropriate user management authorization, authorizing their purpose and use. Authorization will need to be obtained from the Executive Director to ensure that all relevant security policies and requirements are met.

Hardware and software will be checked to ensure that they are compatible with other system components. The use of personal or privately owned information processing

facilities, e.g. laptops, home-computers or hand-held devices, for processing business information, may introduce new vulnerabilities and necessary controls will be identified and implemented.

[Implementation – short term]

Confidentiality agreements

Confidentiality and non-disclosure agreements protect organisational information and inform signatories of their responsibility to protect, use, and disclose information in a responsible and authorised manner. Requirements for confidentiality or non-disclosure agreements reflecting the WCPFC's needs for the protection of information have been identified and are regularly reviewed. The WCPFC's non-disclosure agreements address the requirement to protect the confidentiality of information using legally enforceable terms. To identify requirements for the non-disclosure agreements, the following elements were considered:

k. a definition of the information to be protected (e.g. confidential information);

l. expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;

m. required actions when an agreement is terminated;

n. responsibilities and actions of signatories to avoid unauthorized information disclosure (such as 'need to know');

o. ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;

p. the permitted use of confidential information, and rights of the signatory to use information;

q. the right to audit and monitor activities that involve confidential information;

r. process for notification and reporting of unauthorized disclosure or confidential information breaches;

s. terms for information to be returned or destroyed at agreement cessation; and

t. expected actions to be taken in case of a breach of this agreement.

[Implementation – short term]

Contact with authorities

The WCPFC has procedures in place that specify when and by which authorities (e.g. law enforcement, fire department) will be contacted, and how identified information security incidents will be reported in a timely manner if it is suspected that laws may have been broken.

[Implementation – short term]

Contact with special interest groups with respect to information security

Information sharing agreements will be established to improve cooperation and coordination of security issues. Such agreements will identify requirements for the protection of sensitive information. Membership in special interest groups or forums will be included as a means to:

a. improve knowledge about best practices and staying up to date with relevant security information;

b. ensure the understanding of the information security environment is current and complete;

c. receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities;

d. gain access to specialist information security advice;

e. share and exchange information about new technologies, products, threats, or vulnerabilities; and

f. provide suitable liaison points when dealing with information security incidents.

[Implementation – long term]

Independent review of information security

The WCPFC's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) will be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

[Implementation - long term]

External parties

Any access to the WCPFC sensitive information by external parties needs to be controlled to maintain the security of the information. Controls need to be agreed and defined in an agreement with the external party. External parties include service providers and anyone not an official representative of a CCM.

Identification of risks related to external parties

Sensitive information might be put at risk by external parties with inadequate security management. The risks to the WCPFC's information from external parties needs to be identified and appropriate controls implemented before granting access. The identification of risks related to external party access will include the following:

a. the information processing facilities an external party is required to access;

b. the type of access the external party will have to the information and information processing facilities, e.g.:

1. physical access, e.g. to offices, computer rooms, filing cabinets;
2. logical access, e.g. to a WCPFC's databases, information systems;
3. network connectivity between the WCPFC's and the external party's network(s), e.g. permanent connection, remote access;
4. whether the access is taking place on-site or off-site;

c. the value and sensitivity of the information involved, and its criticality for business operations;

d. the controls necessary to protect information that is not intended to be accessible by external parties;

e. the external party personnel involved in handling the WCPFC's information;

f. how the organization or personnel authorized to have access can be identified, the authorization verified, and how often this needs to be reconfirmed;

g. the different means and controls employed by the external party when storing, processing, communicating, sharing and exchanging information;

h. the impact of access not being available to the external party when required, and the external party entering or receiving inaccurate or misleading information;

i. practices and procedures to deal with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident;

j. legal and regulatory requirements and other contractual obligations relevant to the external party that will be taken into account; and

k. how the interests of any other stakeholders may be affected by the arrangements.

Access by external parties to the WCPFC's information will not be provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. It will be ensured that the external party is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the WCPFC's information.

[Implementation – medium term]

Asset management

The objective of this chapter is to ensure that all assets are accounted for and have a nominated owner.

Responsibility for assets

Owners will be identified for all assets and the responsibility for the maintenance of appropriate controls will be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.

Inventory of assets

All WCPFC assets will be clearly identified and an inventory of all assets drawn up and maintained. The asset inventory will include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets will be identified.

There are many types of assets, including:

a. Physical and electronic information: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;

b. software assets: application software, system software, development tools, and utilities;

c. physical assets: computer equipment, communications equipment, removable media, and other equipment;

d. services: computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning;

e. people, and their qualifications, skills, and experience; and

f. intangibles, such as reputation and image of the WCPFC.

[Implementation – medium term]

Ownership of assets

All information and assets associated with information processing facilities will be owned by a designated part of the WCPFC. The asset owner will be responsible for ensuring that information and assets associated with information processing facilities are appropriately classified and, access restrictions and classifications are periodically reviewed, taking into account applicable access control policies.

[Implementation – medium term]

Acceptable use of assets

All users will follow rules for the acceptable use of information and assets associated with information processing facilities, including rules for electronic mail and Internet usages.

[Implementation – medium term]

Information classification

Information will be classified to indicate the need, priorities, and expected degree of protection when handling the information. Information has varying degrees of sensitivity and criticality. An information classification scheme will be used to define an appropriate set of protection levels and communicate handling measures.

Classification guidelines

Information will be classified in terms of its value, legal requirements, sensitivity, and criticality to the WCPFC. Classifications and associated protective controls for information will take account of business needs for sharing or restricting information and the business impacts associated with such needs. Classification guidelines will include conventions for initial classification and reclassification over time; in accordance with some predetermined access control policy. It is the responsibility of the asset owner to define the classification of an asset, periodically review it, and ensure it is kept up to date and at the appropriate level. Appendix D contains the detailed Information Security Classification Guidelines.

[Implementation – short term]

Information labeling and handling

Procedures for information labeling will cover information assets in physical and electronic formats in accordance with the classification scheme adopted by the WCPFC. Output from systems containing information that is classified as being sensitive or critical will carry an appropriate classification label (in the output). For each classification level, handling procedures including the secure processing, storage, transmission, declassification, and destruction will be defined. This will also include the procedures for chain of custody and logging of any security relevant event. Agreements with other organizations that include information sharing will include procedures to identify the classification of that information and to interpret the classification labels from other organizations.

[Implementation – medium term]

Human resources security

This chapter will ensure that users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of WCPFC facilities and assets.

Prior to employment

The security responsibilities will be addressed prior to employment in adequate job descriptions and in terms and conditions of employment. All candidates for users will be screened. Users of information processing facilities will sign an agreement on their security roles and responsibilities.

Roles and responsibilities

Security roles and responsibilities of users are defined and documented in accordance with the WCPFC's Information Security Policy. Security roles and responsibilities include the requirement to:

a. implement and act in accordance with the WCPFC's ISP;

b. protect assets from unauthorized access, disclosure, modification, destruction or interference;

c. execute particular security processes or activities;

d. ensure responsibility is assigned to the individual for actions taken; and

e. report security events or potential events or other security risks to the WCPFC.

Security roles and responsibilities will be defined and clearly communicated to job candidates during the pre-employment process.

[Implementation – medium term]

Screening

Background verification checks on all candidates for users will be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. Verification checks will take into account all relevant privacy, protection of personal data and/or employment based legislation, and will, where permitted, include the following:

a. availability of satisfactory character references, e.g. one business and one personal;

b. a check (for completeness and accuracy) of the applicant's curriculum vitae;

c. confirmation of claimed academic and professional qualifications;

d. independent identity check (passport or similar document); and

e. more detailed checks, such as credit checks or checks of criminal records.

Information on all candidates being considered for positions within the WCPFC will be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction.

[Implementation – medium term]

Terms and conditions of employment

As part of their contractual obligation, users will agree and sign the terms and conditions of their employment contract, which will state their and the WCPFC's responsibilities for information security. The terms and conditions of employment reflect the WCPFC's security policy in addition to clarifying and stating:

a. that all users who are given access to sensitive information will sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities;

b. the employee's, contractor's and any other user's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation;

c. responsibilities for the classification of information and management of WCPFC assets associated with information systems and services handled by the employee,

d. responsibilities of the user for the handling of information received from other companies or external parties;

e. responsibilities of the WCPFC for the handling of personal information, including personal information created as a result of, or in the course of, employment with the WCPFC;

f. responsibilities that are extended outside the WCPFC's premises and outside normal working hours, e.g. in the case of home-working; and

g. actions to be taken if the user disregards the WCPFC's security requirements.

[Implementation – medium term]

During employment

Management responsibilities will be defined to ensure that security is applied throughout an individual's employment within the WCPFC. An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities will be provided to all users to minimize possible security risks. A formal disciplinary process for handling security breaches will be established.

Management responsibilities

Management will require users to apply security in accordance with established policies and procedures of the WCPFC. Management responsibilities will include ensuring that users:

a. are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information systems;

b. are provided with guidelines to state security expectations of their role within the WCPFC;

c. are motivated to fulfill the security policies of the WCPFC;

d. achieve a level of awareness on security relevant to their roles and responsibilities within the WCPFC;

e. conform to the terms and conditions of employment, which includes the WCPFC's information security policy and appropriate methods of working; and

f. continue to have the appropriate skills and qualifications.

[Implementation – short term]

Information security awareness, education, and training

All employees of the WCPFC and, where relevant, other users will receive appropriate awareness training and regular updates in WCPFC policies and procedures, as relevant for their job function. Awareness training will commence with a formal induction process designed to introduce the WCPFC's security policies and expectations before access to information or services is granted. Ongoing training will include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages and information on the disciplinary process.

[Implementation – medium term]

Disciplinary process

There will be a formal disciplinary process for employees who have committed a security breach. The disciplinary process will not be commenced without prior verification that a security breach has occurred. The formal disciplinary process will ensure correct and fair treatment for employees who are suspected of committing breaches of security. The formal disciplinary process will provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required. In serious cases of misconduct the process will allow for instant removal of duties, access rights and privileges, and for immediate escorting out of the site, if necessary. The disciplinary process will also be used as a deterrent to prevent users in violating WCPFC security policies and procedures, and any other security breaches.

[Implementation – medium term]

Termination or change of employment

Responsibilities will be in place to ensure a user's exit from the WCPFC is managed, and that the return of all equipment and the removal of all access rights are completed. Change of responsibilities and employments within the WCPFC will be managed as the termination of the respective responsibility or employment in line with this section, and any new employments will be managed as described in section 3.1.

Termination responsibilities

The communication of termination responsibilities will include ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement and the terms and conditions of employment continuing for a defined period after the end of the user's employment. Responsibilities and duties still valid after termination of employment will be contained in user's contracts.

[Implementation – medium term]

Return of assets

The termination process will be formalized to include the return of all previously issued software, corporate documents, and equipment. Other WCPFC assets such as mobile computing devices, credit cards, access cards, software, manuals, and information stored on electronic media also will need to be returned. In cases where a user purchases the WCPFC's equipment or uses their own personal equipment, procedures will be followed to ensure that all relevant information is transferred to the WCPFC and securely erased from the equipment.

[Implementation – medium term]

Removal of access rights

Upon termination, the access rights of a user to assets associated with information systems and services will be reconsidered. This will determine whether it is necessary to remove access rights. Changes of employment will be reflected in removal of all access rights that were not approved for the new employment. The access rights that are removed include physical and logical access, keys, identification cards, information processing facilities, subscriptions, and removal from any documentation that identifies them as a current member of the WCPFC. If a departing user has known passwords for accounts remaining active, these will be changed upon termination or change of employment, contract or agreement. Access rights for information assets and information processing facilities will be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

a. whether the termination or change is initiated by the user, or by management and the reason of termination;

b. the current responsibilities of the employee, contractor or any other user; and

c. the value of the assets currently accessible.

[Implementation – short term]

Physical and environmental security

Secure areas

Critical or sensitive information processing facilities will be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They will be physically protected from unauthorized access, damage, and interference. The protection provided will be commensurate with the identified risks.

Physical security perimeter

The following will be implemented where appropriate for physical security perimeters:

a. security perimeters will be clearly defined, and the siting and strength of each of the perimeters will depend on the security requirements of the assets within the perimeter and the results of a risk assessment;

b. perimeters of a building or site containing information processing facilities will be physically sound (i.e. there will be no gaps in the perimeter or areas where a break-in could easily occur); the external walls of the site will be of solid construction and all external doors eill be suitably protected against unauthorized access with control mechanisms, e.g. bars, alarms, locks etc; doors and windows will be locked when unattended;

c. access to sites and buildings will be restricted to authorized personnel only;

d. all fire doors on a security perimeter will be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance to suitable regional, national, and international standards; they will operate in accordance with local fire code in a failsafe manner; and

e. suitable intruder detection systems will be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas will be alarmed at all times.

[Implementation – medium term]

Physical entry controls

The following will be implemented:

a. the date and time of entry and departure of visitors will be recorded, and all visitors will be supervised unless their access has been previously approved; they will only be granted access for specific, authorized purposes and will be issued with instructions on the security requirements of the area and on emergency procedures. access to areas where sensitive information is processed or stored will be controlled and restricted to authorized persons only;

b. authentication controls, e.g. access control card plus PIN, will be used to authorize and validate all access; an audit trail of all access will be securely maintained;

c. all users and all visitors will be required to wear some form of visible identification and will immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;

d. third party support service personnel will be granted restricted access to secure areas or sensitive information processing facilities only when required; this access will be authorized and monitored; and

e. access rights to secure areas will be regularly reviewed and updated, and revoked when necessary.

[Implementation – medium term]

Securing offices, rooms, and facilities

The following will be implemented to secure offices, rooms, and facilities:

a. account will be taken of relevant health and safety regulations and standards;

b. key facilities will be sited to avoid access by the public;

c. where applicable, buildings will be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities; and

d. directories and internal telephone books identifying locations of sensitive information processing facilities will not be readily accessible by the public.

[Implementation – medium term]

Protecting against external and environmental threats

Consideration will be given to any security threats presented by neighboring premises, e.g. a fire in a neighbouring building, water leaking from the roof or in floors below ground level or an explosion in the street. The following will be implemented to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster:

a. hazardous or combustible materials will be stored at a safe distance from a secure area. Bulk supplies such as stationery will not be stored within a secure area;

b. fallback equipment and back-up media will be sited at a safe distance to avoid damage from a disaster affecting the main site; and

c. appropriate fire fighting equipment will be provided and suitably placed.

[Implementation – medium term]

Working in secure areas

Physical protection and guidelines for working in secure areas will be designed and applied. The following will be implemented:

a. personnel will only be aware of the existence of, or activities within, a secure area on a need to know basis;

b. unsupervised working in secure areas will be avoided both for safety reasons and to prevent opportunities for malicious activities;

c. vacant secure areas will be physically locked and periodically checked; and

d. photographic, video, audio or other recording equipment, such as cameras in mobile devices, will not be allowed, unless authorized.

[Implementation – medium term]

Public access, delivery, and loading areas

Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises will be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. The following will be implemented:

a. access to a delivery and loading area from outside of the building will be restricted to identified and authorized personnel;
b. the delivery and loading area will be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building;
c. the external doors of a delivery and loading area will be secured when the internal doors are opened;
d. incoming material will be inspected for potential threats before this material is moved from the delivery and loading area to the point of use; and
e. incoming material will be registered in accordance with asset management procedures on entry to the site.

[Implementation – medium term]

Equipment security

Equipment will be protected from physical and environmental threats. Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. This will also consider equipment placement and disposal.

Equipment placement and protection

Equipment will be placed to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. The following will be implemented to protect equipment:

a. equipment will be placed to minimize unnecessary access into work areas;

b. information processing facilities handling sensitive data will be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access;

c. controls will be adopted to minimize the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water, dust, vibration, chemical effects, electrical supply interference, communications interference, and vandalism;

d. guidelines for eating, drinking, and smoking in proximity to information processing facilities will be established;

e. environmental conditions, such as temperature and humidity, will be monitored for conditions, which could adversely affect the operation of information processing facilities; and

f. lightning protection will be applied to all buildings.

[Implementation – medium term]

Supporting utilities

Equipment will be protected from power failures and other disruptions caused by failures in supporting utilities. All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning will be adequate for the systems they are supporting. Support utilities will be regularly inspected and as appropriate tested to ensure their proper functioning and to reduce any risk from their malfunction or failure. A suitable electrical supply will be provided that conforms to the equipment manufacturer's specifications. An uninterruptible power supply (UPS) to support orderly close down or continuous running will be used for equipment supporting critical business operations. Power contingency plans will cover the action to be taken on failure of the UPS. UPS equipment will be regularly checked to ensure it has adequate capacity and is tested in accordance with the manufacturer's recommendations. The water supply will be stable and adequate to supply air conditioning, humidification equipment and fire suppression systems (where used).

[Implementation – medium term]

Cabling security

Power and telecommunications cabling carrying data or supporting information services will be protected from interception or damage. The following will be implemented for cabling security:

a. power cables will be segregated from communications cables to prevent interference;

b. clearly identifiable cable and equipment markings will be used to minimise handling errors, such as accidental patching of wrong network cables; and

c. a documented patch list will be used to reduce the possibility of errors.

[Implementation – medium term]

Equipment maintenance

Equipment will be correctly maintained to ensure its continued availability and integrity. The following will be implemented for equipment maintenance:

a. equipment will be maintained in accordance with the supplier's recommended service intervals and specifications;

b. only authorized maintenance personnel will carry out repairs and service equipment;

c. records will be kept of all suspected or actual faults, and all preventive and corrective maintenance;

d. appropriate controls will be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the WCPFC; and

e. all requirements imposed by insurance policies will be complied with.

[Implementation – medium term]

Security of equipment off-premises

Security will be applied to off-site equipment. Regardless of ownership, the use of any information processing equipment outside the WCPFC's premises will need to be authorized by management. The following will be implemented for the protection of off-site equipment:

a. equipment and media taken off the premises will not be left unattended in public places; portable computers will be carried as hand luggage when traveling;

b. manufacturers' instructions for protecting equipment will be observed at all times;

c. home-working controls will be determined by a risk assessment and suitable controls applied as appropriate; and

d. adequate insurance cover will need to be in place to protect equipment off-site.

[Implementation – medium term]

Secure disposal or re-use of equipment

All items of equipment containing storage media will be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. Devices containing sensitive information will be physically destroyed or the information will be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function. Damaged devices containing sensitive data will require a risk assessment to determine whether the items will be physically destroyed rather than sent for repair or discarded.

[Implementation – medium term]

Removal of property

Equipment, information or software will not be taken off-site without prior authorization. The following will be implemented:

a. equipment, information or software will not be taken off-site without prior authorization;

b. users who have authority to permit off-site removal of assets will be clearly identified;

c. time limits for equipment removal will be set and returns checked for compliance; and

d. equipment will be recorded as being removed off-site and recorded when returned.

[Implementation – medium term]

Communications and operations management

Operational procedures and responsibilities

Responsibilities and procedures for the management and operation of all information processing facilities will be established. This is to ensure the correct and secure operation of these facilities.

Documented operating procedures

Operating procedures will be documented, maintained, and made available to all users who need them. Documented procedures will be prepared for system activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management, and safety. The operating procedures will specify the instructions for the detailed execution of each job including:

a. processing and handling of information;

b. backup;

c. scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;

d. instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;

e. support contacts in the event of unexpected operational or technical difficulties;

f. special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output;

g. system restart and recovery procedures; and

h. the management of audit-trail and system log information.

[Implementation – medium term]

Change management

Operational systems and application software will be subject to strict change management control**.** The following will be implemented:

a. identification and recording of significant changes;

b. planning and testing of changes;

c. assessment of the potential impacts, including security impacts, of such changes;

d. formal approval procedure for proposed changes;

e. communication of change details to all relevant persons;

f. fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

Formal management responsibilities and procedures will be in place to ensure satisfactory control of all changes to equipment, software or procedures. When changes are made, an audit log containing all relevant information will be retained. Changes to operational systems will only be made when there is a valid business reason to do so, such as an increase in the risk to the system. Updating systems with the latest versions of operating system or application is not always in the business interest as this could introduce more vulnerabilities and instability than the current version. There may also be a need for additional training, license costs, support, maintenance and administration overhead, and new hardware especially during migration.

[Implementation – medium term]

Segregation of duties

Duties and areas of responsibility will be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the WCPFC's assets. Care will be taken that no single person can access, modify or use assets without authorization or detection. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision will be considered.

[Implementation – medium term]

Separation of development, test, and operational facilities

Development, test, and operational facilities will be separated to reduce the risks of unauthorized access or changes to the operational system. In particular, the following items will be considered:

a. rules for the transfer of software from development to operational status will be defined and documented;

b. development and operational software will run on different systems or computer processors and in different domains or directories;

c. compilers, editors, and other development tools or system utilities will not be accessible from operational systems when not required;

d. the test system environment will emulate the operational system environment as closely as possible;

e. users will use different user profiles for operational and test systems, and menus will display appropriate identification messages to reduce the risk of error; and

f. sensitive data will not be copied into the test system environment.

[Implementation – long term]

Third party service delivery management

The WCPFC will check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party.

Service delivery

WCPFC will ensure that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party. Service delivery by a third party will include the agreed security arrangements, service definitions, and aspects of service management. In case of outsourcing arrangements, the WCPFC will plan the necessary transitions (of information, information processing facilities, and anything else that needs to be moved), and will ensure that security is maintained throughout the transition period. The WCPFC will ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

[Implementation – medium term]

Monitoring and review of third party services

The services, reports and records provided by the third party will be regularly monitored and reviewed, and audits will be carried out regularly. Monitoring and review of third party services will ensure that the information security terms and conditions of the agreements are being adhered to, and that information security incidents and problems are managed properly. This will involve a service management relationship and process between the WCPFC and the third party to:

a. monitor service performance levels to check adherence to the agreements;

b. review service reports produced by the third party and arrange regular progress meetings as required by the agreements;

c. provide information about information security incidents and review of this information by the third party and the WCPFC as required by the agreements and any supporting guidelines and procedures;

d. review third party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered; and

e. resolve and manage any identified problems.

[Implementation – medium term]

Managing changes to third party services

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, will be managed, taking account

of the criticality of business systems and processes involved and re-assessment of risks. The process of managing changes to a third party service will take account of:

a. changes made by the WCPFC to implement:
    i. enhancements to the current services offered;
    ii. development of any new applications and systems;
    iii. modifications or updates of the WCPFC's policies and procedures; and
    iv. new controls to resolve information security incidents and to improve security;
b. changes in third party services to implement:
    i. changes and enhancement to networks;
    ii. use of new technologies;
    iii. adoption of new products or newer versions/releases;
    iv. new development tools and environments;
    v. changes to physical location of service facilities; and
    vi. change of vendors.

[Implementation – medium term]

System planning and acceptance

Advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance. Projections of future capacity requirements will be made, to reduce the risk of system overload. The operational requirements of new systems will be established, documented, and tested prior to their acceptance and use.

Capacity management

The use of resources will be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

[Implementation – long term]

System acceptance

Acceptance criteria for new information systems, upgrades, and new versions will be established and suitable tests of the system(s) carried out during development and prior to acceptance. Managers will ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested. New information systems, upgrades, and new versions will only be migrated into production after obtaining formal acceptance. The following items will be considered prior to formal acceptance being provided:

a. performance and computer capacity requirements;

b. error recovery and restart procedures, and contingency plans;

c. preparation and testing of routine operating procedures to defined standards;

d. agreed set of security controls in place;

e. effective manual procedures;

f. business continuity arrangements;

g. evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end;

h. evidence that consideration has been given to the effect the new system has on the overall security of the WCPFC;

i. training in the operation or use of new systems; and

j. ease of use, as this affects user performance and avoids human error.

[Implementation – long term]

Protection against malicious and mobile code

Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code. Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users will be made aware of the dangers of malicious code. Managers will introduce controls to prevent, detect, and remove malicious code and control mobile code.

Controls against malicious code

Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures will be implemented. Protection against malicious code will be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls. The following will be implemented:

c. establishing a formal policy prohibiting the use of unauthorized software;

d. establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures will be taken;

e. conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments will be formally investigated;

f. installation and regular update of malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the checks carried out will include:

i. checking any files on electronic or optical media, and files received over networks, for malicious code before use;

ii. checking electronic mail attachments and downloads for malicious code before use; this check will be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the WCPFC; and

iii. checking web pages for malicious code;

g. defining management procedures and responsibilities to deal with malicious code protection on systems, training in their use, reporting and recovering from malicious code attacks;

h. preparing appropriate business continuity plans for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements;

i. implementing procedures to regularly collect information, such as subscribing to mailing lists and/or checking web sites giving information about new malicious code; and

j. implementing procedures to verify information relating to malicious code, and ensure that warning bulletins are accurate and informative; managers will ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malicious code, are used to differentiate between hoaxes and real malicious code; all users will be made aware of the problem of hoaxes and what to do on receipt of them.

[Implementation – short to medium term]

Controls against mobile code

Mobile code is software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction. Mobile code is associated with a number of middleware services. Where the use of mobile code is authorized, the configuration will ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code will be prevented from executing. The following actions will be implemented to protect against mobile code performing unauthorized actions:

a. executing mobile code in a logically isolated environment;

b. blocking any unauthorized use of mobile code;

c. blocking any unauthorized receipt of mobile code;

d. activating technical measures as available on a specific system to ensure mobile code is managed;

e. control the resources available to mobile code access; and

f. cryptographic controls to uniquely authenticate mobile code.

[Implementation – long term]

Back-up

Routine procedures will be established to implement the agreed back-up policy and strategy for taking back-up copies of data and rehearsing their timely restoration.

Information back-up

Back-up copies of information and software will be taken and tested regularly in accordance with the agreed backup policy. Adequate back-up facilities will be provided to ensure that all essential information and software can be recovered following a disaster or media failure. The following items for information back up will be implemented:

a. the necessary level of back-up information will be defined;

b. accurate and complete records of the back-up copies and documented restoration procedures will be produced;

c. the extent (e.g. full or differential backup) and frequency of backups will reflect the business requirements of the WCPFC, the security requirements of the information involved, and the criticality of the information to the continued operation of the WCPFC;

d. the back-ups will be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;

e. back-up information will be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site; the controls applied to media at the main site will be extended to cover the back-up site;

f. back-up media will be regularly tested to ensure that they can be relied upon for emergency use when necessary;

g. restoration procedures will be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery; and

h. in situations where confidentiality is of importance, back-ups will be protected by means of encryption.

[Implementation – long term]

Network security management

The secure management of networks, which may span WCPFC boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection. Additional controls may also be required to protect sensitive information passing over public networks.

Network controls

Networks will be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. Network managers will implement controls to ensure the security of information in networks, and the protection of connected services from unauthorized access. In particular, the following items will be implemented:

a. special controls will be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks;

b. appropriate logging and monitoring will be applied to enable recording of security relevant actions; and

c. management activities will be closely co-ordinated both to optimize the service to the WCPFC and to ensure that controls are consistently applied across the information processing infrastructure.

[Implementation – short term]

Security of network services

Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls and intrusion detection systems. Security features, service levels, and management requirements of all network services will be identified and included in any network services agreement, whether these services are provided in-house or outsourced. The ability of the network service provider to manage agreed services in a secure way will be determined and regularly monitored, and the right to audit will be agreed. The security arrangements necessary for particular services, such as security features, service levels, and management requirements, will be identified. The WCPFC will ensure that network service providers implement these measures.

[Implementation – long term]

Media handling

Media will be controlled and physically protected. Appropriate operating procedures will be established to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.

Management of removable media

Removable media include tapes, disks, flash disks, removable hard drives, CDs, DVDs, and printed media. There will be procedures in place for the management of removable media. The following will be implemented for the management of removable media:

a. if no longer required, the contents of any re-usable media will be made unrecoverable;

b. authorization will be required for media removed from the WCPFC and a record of such removals will be kept in order to maintain an audit trail; and

c. all media will be stored in a safe, secure environment, in accordance with manufacturers' specifications;

[Implementation – medium term]

Disposal of media

Formal procedures for the secure disposal of media will minimize the risk of sensitive information leakage to unauthorised persons. The procedures for secure disposal of media containing sensitive information will be commensurate with the sensitivity of that information. The following items will be implemented:

a. media containing sensitive information will be stored and disposed of securely and safely;

b. procedures will be in place to identify the items that might require secure disposal; and

c. disposal of sensitive items will be logged in order to maintain an audit trail.

[Implementation – medium term]

Information handling procedures

Procedures will be drawn up for handling, processing, storing, and communicating information consistent with its classification. The following items will be implemented:

a. handling and labelling of all media to its indicated classification level;

b. access restrictions to prevent access from unauthorized personnel;

c. maintenance of a formal record of the authorized recipients of data;

d. ensuring that input data is complete, that processing is properly completed and that output validation is applied;

e. storage of media in accordance with manufacturers' specifications; and

f. review of distribution lists and lists of authorized recipients at regular intervals.

[Implementation – medium term]

Security of system documentation

System documentation will be protected against unauthorized access. To secure system documentation, the following items will be implemented:

a. system documentation will be stored securely; and

b. the access list for system documentation will be kept to a minimum and authorized by the application owner.

[Implementation – long term]

Exchange of information

Exchanges of information and software between organizations will be based on a formal exchange policy, carried out in line with exchange agreements, and will be compliant with any relevant legislation. Procedures and standards will be established to protect information and physical media containing information in transit.

Information exchange policies and procedures

Formal exchange policies, procedures, and controls will be in place to protect the exchange of information through the use of all types of communication facilities. The procedures and controls to be followed when using electronic communication facilities for information exchange will include the following items:

a. procedures designed to protect exchanged information from interception, copying, modification, mis-routing, and destruction;

b. procedures for the detection of and protection against malicious code that may be transmitted through the use of electronic communications;

c. procedures for protecting communicated sensitive electronic information that is in the form of an attachment;

d. policy outlining acceptable use of electronic communication facilities;

e. procedures for the use of wireless communications;

f. employee, contractor and any other user's responsibilities not to compromise the WCPFC, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.;

g. use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information;

h. retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations;

i. not leaving sensitive or critical information on printing facilities, e.g. copiers, printers, and facsimile machines, as these may be accessed by unauthorized personnel;

j. controls and restrictions associated with the forwarding of communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses;

k. reminding personnel that they need to take appropriate precautions, e.g. not to reveal sensitive information to avoid being overheard or intercepted when making a phone call by:

    i. people in their immediate vicinity particularly when using mobile phones;

    ii. wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers; and

    iii. people at the recipient's end;

l. not leaving messages containing sensitive information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialing;

m. reminding personnel about the problems of using facsimile machines, namely:

    i. unauthorized access to built-in message stores to retrieve messages;

    ii. deliberate or accidental programming to send messages to specific numbers; and

    iii. sending documents and messages to the wrong number either by misdialing or using the wrong stored number;

n. reminding personnel not to register demographic data, such as the e-mail address or other personal information, in any software to avoid collection for unauthorized use; and

o. reminding personnel that modern facsimile machines and photocopiers have page caches and store pages in case of a paper or transmission fault, which will be printed once the fault is cleared.

[Implementation – medium term]

Exchange agreements

Agreements will be established for the exchange of information and software between the WCPFC and external parties. Policies, procedures, and standards will be established and maintained to protect information and physical media in transit, and will be referenced in such exchange agreements. The security content of the agreement will reflect the sensitivity of the information involved. Exchange agreements will include the following security conditions:

a. management responsibilities for controlling and notifying transmission, dispatch, and receipt;

b. procedures for notifying sender of transmission, dispatch, and receipt;

c. procedures to ensure traceability and non-repudiation;

d. minimum technical standards for packaging and transmission;

e. escrow agreements;

f. courier identification standards;

g. responsibilities and liabilities in the event of information security incidents, such as loss of data;

h. use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected;

i. ownership and responsibilities for data protection, copyright, software license compliance and similar considerations; and

j. technical standards for recording and reading information and software.

[Implementation – medium term]

Physical media in transit

Media containing information will be protected against unauthorized access, misuse or corruption during transportation beyond WCPFC's physical boundaries. The following will be implemented to protect information media being transported between sites:

a. reliable transport or couriers will be used;

b. a list of authorized couriers will be agreed with management;

c. procedures to check the identification of couriers will be developed;

d. packaging will be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications (e.g. for software), for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields;

e. controls will be adopted to protect sensitive information from unauthorized disclosure or modification; examples include:

    i. use of locked containers;

    ii. delivery by hand;

    iii. tamper-evident packaging (which reveals any attempt to gain access); and

    iv. in exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes.

[Implementation – medium term]

Electronic messaging

Information involved in electronic messaging will be appropriately protected. Security considerations for electronic messaging will include the following:

a. protecting messages from unauthorized access, modification or denial of service;

b. ensuring correct addressing and transportation of the message;

c. general reliability and availability of the service;

d. legal considerations, for example requirements for electronic signatures;

e. obtaining approval prior to using external public services such as instant messaging or file sharing; and

f. stronger levels of authentication controlling access from publicly accessible networks.

[Implementation – medium term]

Business information systems

Policies and procedures will be developed and implemented to protect information associated with the interconnection of business information systems. Consideration given to the security and business implications of interconnecting such facilities will include:

a. known vulnerabilities in the administrative and accounting systems where information is shared between different parts of the WCPFC;

b. vulnerabilities of information in business communication systems, e.g. recording phone calls or conference calls, confidentiality of calls, storage of facsimiles, opening mail, distribution of mail;

c. policy and appropriate controls to manage information sharing;

d. excluding categories of sensitive business information and classified documents if the system does not provide an appropriate level of protection;

e. restricting access to diary information relating to selected individuals, e.g. personnel working on sensitive projects;

f. categories of personnel, contractors or business partners allowed to use the system and the locations from which it may be accessed;

g. restricting selected facilities to specific categories of user;

h. retention and back-up of information held on the system; and

i. fallback requirements and arrangements.

[Implementation – medium term]

Electronic commerce services

The security implications associated with using electronic commerce services, including on-line transactions, and the requirements for controls, will be implemented. The integrity and availability of information electronically published through publicly available systems will also be considered.

Electronic commerce

Information involved in electronic commerce passing over public networks will be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. Security considerations for electronic commerce will include the following:

a. the level of confidence each party requires in each others claimed identity, e.g. through authentication;

b. authorization processes associated with who may set prices, issue or sign key trading documents;

c. ensuring that trading partners are fully informed of their authorisations;

d. determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents, and the non-repudiation of contracts, e.g. associated with tendering and contract processes;

e. the level of trust required in the integrity of advertised price lists;

f. the confidentiality of any sensitive data or information;

g. the confidentiality and integrity of any order transactions, payment information, delivery address details, and confirmation of receipts;

h. the degree of verification appropriate to check payment information supplied by a customer;

i. selecting the most appropriate settlement form of payment to guard against fraud;

j. the level of protection required to maintain the confidentiality and integrity of order information;

k. avoidance of loss or duplication of transaction information;

l. liability associated with any fraudulent transactions; and

m. insurance requirements.

[Implementation – long term]

On-Line Transactions

Information involved in on-line transactions will be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. Security considerations for on-line transactions will include the following:

a. the use of electronic signatures by each of the parties involved in the transaction;

b. all aspects of the transaction, i.e. ensuring that:

    i. user credentials of all parties are valid and verified;

    ii. the transaction remains confidential; and

    iii. privacy associated with all parties involved is retained;

c. communications path between all involved parties is encrypted;

d. protocols used to communicate between all involved parties is secured;

e. ensuring that the storage of the transaction details are located outside of any public accessible environment, e.g. on a storage platform existing on the WCPFC's Intranet, and not retained and exposed on a storage medium directly accessible from the Internet; and

f. where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures and/or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process.

[Implementation – long term]

Publicly available information

The integrity of information being made available on a publicly available system will be protected to prevent unauthorized modification. Software, data, and other information requiring a high level of integrity, being made available on a publicly available system, will be protected by appropriate mechanisms, e.g. digital signatures. The publicly accessible system will be tested against weaknesses and failures prior to information being made available. There will be a formal approval process before information is made publicly available. In addition, all input provided from the outside to the system will be verified and approved. Electronic publishing systems, especially those that permit feedback and direct entering of information, will be carefully controlled so that:

a. information is obtained in compliance with any data protection legislation;

b. information input to, and processed by, the publishing system will be processed completely and accurately in a timely manner;

c. sensitive information will be protected during collection, processing, and storage; and

d. access to the publishing system does not allow unintended access to networks to which the system is connected.

[Implementation – long term]

Monitoring

Systems will be monitored and information security events will be recorded. Operator logs and fault logging will be used to ensure information system problems are identified. WCPFC will comply with all relevant legal requirements applicable to its monitoring and logging activities. System monitoring will be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

Audit logging

Audit logs recording user activities, exceptions, and information security events will be produced and kept for an agreed period to assist in future investigations and access control monitoring. Audit logs will include, when relevant:

a. user IDs;

b. dates, times, and details of key events, e.g. log-on and log-off;

c. terminal identity or location;

d. records of successful and rejected system access attempts;

e. records of successful and rejected data and other resource access attempts;

f. changes to system configuration;

g. use of privileges;

h. use of system utilities and applications;

i. files accessed and the kind of access;

j. network addresses and protocols;

k. alarms raised by the access control system; and

l. activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.

[Implementation – medium term]

Monitoring system use

Procedures for monitoring use of information processing facilities will be established and the results of the monitoring activities reviewed regularly. The level of monitoring required for individual facilities will be determined by a risk assessment. WCPFC will comply with all relevant legal requirements applicable to its monitoring activities. Areas that will be implemented include:

a. authorized access, including detail such as:
    i. the user ID;
    ii. the date and time of key events;
    iii. the types of events;
    iv. the files accessed;
    v. the program/utilities used;

b. all privileged operations, such as:
    i. use of privileged accounts, e.g. supervisor, root, administrator;
    ii. system start-up and stop;
    iii. I/O device attachment/detachment;

c. unauthorized access attempts, such as:
    i. failed or rejected user actions;
    ii. failed or rejected actions involving data and other resources;
    iii. access policy violations and notifications for network gateways and firewalls;
    iv. alerts from proprietary intrusion detection systems;

d. system alerts or failures such as:
    i. console alerts or messages;
    ii. system log exceptions;
    iii. network management alarms;
    iv. alarms raised by the access control system;

e. changes to, or attempts to change, system security settings and controls.

How often the results of monitoring activities are reviewed will depend on the risks involved. Risk factors that will be considered include the:

a. criticality of the application processes;

b. value, sensitivity, and criticality of the information involved;

c. past experience of system infiltration and misuse, and the frequency of vulnerabilities being exploited;

d. extent of system interconnection (particularly public networks); and

e. logging facility being de-activated.

[Implementation – long term]

Protection of log information

Logging facilities and log information will be protected against tampering and unauthorized access. Controls will protect against unauthorized changes and operational problems with the logging facility including:

a. alterations to the message types that are recorded;

b. log files being edited or deleted; and

c. storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

[Implementation – long term]

Administrator and operator logs

System administrator and system operator activities will be logged. Logs will include:

a. the time at which an event (success or failure) occurred;

b. information about the event (e.g. files handled) or failure (e.g. error occurred and

c. corrective action taken);

d. which account and which administrator or operator was involved; and

e. which processes were involved.

[Implementation – medium term]

Fault logging

Faults reported by users or by system programs related to problems with information processing or communications systems will be logged. There will be clear rules for handling reported faults including:

c. review of fault logs to ensure that faults have been satisfactorily resolved; and

d. review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized.

[Implementation – short term]

Clock synchronization

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. Therefore, where a computer or communications device has the capability to operate a real-time clock, this clock will be set to an agreed standard. As some clocks are known to drift with time, there will be a procedure that checks for and corrects any significant variation. The correct interpretation of the date/time format is important to ensure that the timestamp reflects the real date/time. Local specifics (e.g. daylight savings) will be taken into account.

[Implementation – medium term]

Access control

Business requirement for access control

Access to information, information processing facilities, and business processes will be controlled on the basis of business and security requirements. Access control rules will take account of policies for information dissemination and authorization.

Access control policy

An access control policy will be established, documented, and reviewed based on business and security requirements for access. Access control rules and rights for each user or group of users will be clearly stated in an access control policy. Access controls are both logical and physical and these will be considered together. Users and service providers will be given a clear statement of the business requirements to be met by access controls. The policy will include the following:

a. security requirements of individual business applications;

b. identification of all information related to the business applications and the risks the information is facing;

c. policies for information dissemination and authorization, e.g. the need to know principle and security levels and classification of information;

d. consistency between the access control and information classification policies of different systems and networks;

e. relevant legislation and any contractual obligations regarding protection of access to data or services;

f. standard user access profiles for common job roles in the WCPFC;

g. management of access rights in a distributed and networked environment which recognizes all types of connections available;

h. segregation of access control roles, e.g. access request, access authorization, access administration;

i. requirements for formal authorization of access requests;

j. requirements for periodic review of access controls; and

k. removal of access rights.

[Implementation – medium term]

User access management

Formal procedures will be in place to control the allocation of access rights to information systems and services. The procedures will cover all stages in the life-cycle of

user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.

User registration

There will be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. The access control procedure for user registration and de-registration will include:

a. using unique user IDs to enable users to be linked to and held responsible for their actions;

b. the use of group IDs will only be permitted where they are necessary for business or operational reasons, and will be approved and documented;

c. checking that the user has authorization from the system owner for the use of the information system or service;

d. checking that the level of access granted is appropriate to the business purpose and is consistent with the WCPFC security policy;

e. giving users a written statement of their access rights;

f. requiring users to sign statements indicating that they understand the conditions of access;

g. ensuring service providers do not provide access until authorization procedures have been completed;

h. maintaining a formal record of all persons registered to use the service;

i. immediately removing or blocking access rights of users who have changed roles or jobs or left the WCPFC;

j. periodically checking for, and removing / blocking, redundant user IDs and accounts; and

k. ensuring that redundant user IDs are not issued to users.

[Implementation – medium term]

Privilege management

The allocation and use of privileges will be restricted and controlled. Multi-user systems that require protection against unauthorized access will have the allocation of privileges controlled through a formal authorization process. The following steps will be implemented:

d. the access privileges associated with each computer system will be identified;

e. privileges will be allocated to users on a need-to-use basis in line with the access control policy i.e. the minimum requirement for their functional role only when needed; and

f. an authorization process and a record of all privileges allocated will be maintained. Privileges will not be granted until the authorization process is complete.

[Implementation – short term]

User password management

The allocation of passwords will be controlled through a formal management process. The process will include the following requirements:

i. users will be required to sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group; this signed statement could be included in the terms and conditions of employment;

j. when users are required to maintain their own passwords they will be provided initially with a secure temporary password, which they are forced to change immediately;

k. establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password;

l. temporary passwords will be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages will be avoided;

m. temporary passwords will be unique to an individual and will not be guessable;

n. users will acknowledge receipt of passwords;

o. passwords will never be stored on computer systems in an unprotected form; and

p. default vendor passwords will be altered following installation of systems or software.

[Implementation – short term]

Review of user access rights

Management will review users' access rights at regular intervals using a formal process. The review of access rights will consider the following:

a. users' access rights will be reviewed every year, and after any changes, such as promotion, demotion, or termination of employment;

b. authorizations for special privileged access rights will be reviewed every 3 months;

c. privilege allocations will be checked at regular intervals to ensure that unauthorized privileges have not been obtained; and

d. changes to privileged accounts will be logged for periodic review.

[Implementation – medium term]

User responsibilities

The co-operation of authorized users is essential for effective security. Users will be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment. A clear desk and clear screen policy will be implemented to reduce the risk of unauthorized access or damage to papers, media, and information processing facilities.

Password use

Users will be required to follow good security practices in the selection and use of passwords. All users will be advised to:

j. keep passwords confidential;

k. avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved;

l. change passwords whenever there is any indication of possible system or password compromise;

m. select quality passwords with sufficient minimum length which are:

   i. easy to remember;

   ii. not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;

   iii. not vulnerable to dictionary attacks (do not consist of words included in dictionaries);

   iv. free of consecutive identical, all-numeric or all-alphabetic characters;

n. change passwords at regular intervals (passwords for privileged accounts will be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;

o. change temporary passwords at the first log-on;

p. not include passwords in any automated log-on process, e.g. stored in a macro or function key;

q. not share individual user passwords; and

r. not use the same password for business and non-business purposes.

[Implementation – short term]

Unattended user equipment

Users will ensure that unattended equipment has appropriate protection. All users will be made aware of the security requirements and procedures for protecting unattended

equipment, as well as their responsibilities for implementing such protection. Users will be advised to:

a. terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;

b. log-off servers, and office PCs when the session is finished; and

c. secure PCs or terminals from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

[Implementation – medium term]

Clear desk and clear screen policy

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities will be adopted. The clear desk and clear screen policy will take into account the information classifications, legal and contractual requirements, and the corresponding risks and cultural aspects of the WCPFC. The following guidelines will be implemented:

a. sensitive or critical business information, e.g. on paper or on electronic storage media, will be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated;

b. computers and terminals will be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and will be protected by key locks, passwords or other controls when not in use;

c. incoming and outgoing mail points and unattended facsimile machines will be protected;

d. unauthorised use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) will be prevented; and

e. documents containing sensitive or classified information will be removed from printers immediately.

[Implementation – long term]

Network access control

Access to both internal and external networked services will be controlled. User access to networks and network services will not compromise the security of the network services by ensuring that: appropriate interfaces are in place between the WCPFC's network and networks owned by other organizations, and public networks; appropriate authentication mechanisms are applied for users and equipment; and control of user access to information services in enforced.

Policy on use of network services

Users will only be provided with access to the services that they have been specifically authorized to use. A policy will be formulated concerning the use of network services and will cover:

a. the network services which are allowed to be accessed;

b. authorization procedures for determining who is allowed to access which networked services;

c. management controls and procedures to protect access to network services; and

d. the means used to access network services (e.g. the conditions for allowing dial-up access to an Internet service provider or remote system).

[Implementation – medium term]

User authentication for external connections

Appropriate authentication methods will be used to control access by remote users. Authentication of remote users can be achieved using, for example, a cryptographic based technique, hardware tokens, or a challenge/response protocol. Additional authentication controls will be implemented to control access to wireless networks. In particular, special care is needed in the selection of controls for wireless networks due to the greater opportunities for undetected interception and insertion of network traffic.

[Implementation – short term]

Equipment identification in networks

Automatic equipment identification will be implemented as a means to authenticate connections from specific locations and equipment. An identifier in or attached to, the equipment can be used to indicate whether this equipment is permitted to connect to the network. These identifiers will clearly indicate to which network the equipment is permitted to connect.

[Implementation – long term]

Remote diagnostic and configuration port protection

Physical and logical access to diagnostic and configuration ports will be controlled. Potential controls for the access to diagnostic and configuration ports include the use of a key lock and supporting procedures to control physical access to the port. Ports, services, and similar facilities installed on a computer or network, which are not specifically required for business functionality, will be disabled or removed.

[Implementation – medium term]

Segregation in networks

Groups of information services, users, and information systems will be segregated on networks. The criteria for segregation of networks into domains will be based on the access control policy and access requirements, and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology.

[Implementation – long term]

Network connection control

For shared networks, especially those extending across the WCPFC's boundaries, the capability of users to connect to the network will be restricted, in line with the access control policy and requirements of the business applications. The network access rights of users will be maintained and updated as required by the access control policy. Examples of applications to which restrictions will be applied are:

a. messaging, e.g. electronic mail;

b. file transfer;

c. interactive access; and

d. application access.

[Implementation – long term]

Network routing control

Routing controls will be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. Routing controls will be based on positive source and destination address checking mechanisms. The requirements for network routing control will be based on the access control policy.
[Implementation – long term]

Operating system access control

Security facilities will be used to restrict access to operating systems to authorized users. The facilities will be capable of the following:

g. authenticating authorized users, in accordance with a defined access control policy;

h. recording successful and failed system authentication attempts;

i. recording the use of special system privileges;

j. issuing alarms when system security policies are breached;

k. providing appropriate means for authentication; and

l. where appropriate, restricting the connection time of users.

Secure log-on procedures

Access to operating systems will be controlled by a secure log-on procedure. The procedure for logging into an operating system will be designed to minimize the opportunity for unauthorized access. The log-on procedure will therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance. A good log-on procedure will:

a. not display system or application identifiers until the log-on process has been successfully completed;

b. display a general notice warning that the computer will only be accessed by authorized users;

c. not provide help messages during the log-on procedure that would aid an unauthorized user;

d. validate the log-on information only on completion of all input data. If an error condition arises, the system will not indicate which part of the data is correct or incorrect;

e. limit the number of unsuccessful log-on attempts allowed to three attempts, and:

    i. record unsuccessful and successful attempts;

    ii. force a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorization;

    iii. disconnect data link connections;

    iv. send an alarm message to the system console if the maximum number of log-on attempts is reached;

    v. set the number of password retries in conjunction with the minimum length of the password and the value of the system being protected;

f. limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system will terminate the log-on;

g. display the following information on completion of a successful log-on:

    i. date and time of the previous successful log-on;

    ii. details of any unsuccessful log-on attempts since the last successful log-on;

h. not display the password being entered or hide the password characters by symbols; and

i. not transmit passwords in clear text over a network.

[Implementation – medium term]

User identification and authentication

All users will have a unique identifier (user ID) for their personal use only, and a suitable authentication technique will be chosen to substantiate the claimed identity of a user. This control will be applied for all types of users. User IDs will be used to trace activities to the responsible individual. Regular user activities will not be performed from privileged accounts.

[Implementation – short term]

Password management system

Systems for managing passwords will be interactive and will ensure quality passwords. A password management system will:

a. enforce the use of individual user IDs and passwords to maintain accountability;

b. allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;

c. enforce a choice of quality passwords;

d. enforce password changes;

e. force users to change temporary passwords at the first log-on;

f. maintain a record of previous user passwords and prevent re-use;

g. not display passwords on the screen when being entered;

h. store password files separately from application system data; and

i. store and transmit passwords in protected (e.g. encrypted or hashed) form.

[Implementation – medium term]

Use of system utilities

The use of utility programs that might be capable of overriding system and application controls will be restricted and tightly controlled. The following will be implemented:

a. use of identification, authentication, and authorization procedures for system utilities;

b. segregation of system utilities from applications software;

c. limitation of the use of system utilities to the minimum practical number of trusted, authorized users;

d. authorization for ad hoc use of systems utilities;

e. limitation of the availability of system utilities, e.g. for the duration of an authorized change;

f. logging of all use of system utilities;

g. defining and documenting of authorization levels for system utilities;

h. removal or disabling of all unnecessary software based utilities and system software; and

i. not making system utilities available to users who have access to applications on systems where segregation of duties is required.

[Implementation – medium term]

Session time-out

Inactive sessions will shut down after a defined period of inactivity. A time-out facility will clear the session screen and also, possibly later, close both application and network sessions after a defined period of inactivity. The time-out delay will reflect the security risks of the area, the classification of the information being handled and the applications being used, and the risks related to the users of the equipment.

[Implementation – medium term]

Limitation of connection time

Restrictions on connection times will be used to provide additional security for high-risk applications. Examples of such restrictions include:

a. using predetermined time slots or regular interactive sessions of short duration;

b. restricting connection times to normal office hours; and

c. considering re-authentication at timed intervals.

[Implementation – long term]

Application and information access control

Security facilities will be used to restrict access to and within application systems. Logical access to application software and information will be restricted to authorized users. Application systems will:

a. control user access to information and application system functions, in accordance with a defined access control policy;

b. provide protection from unauthorized access by any utility, operating system software, and malicious software that is capable of overriding or bypassing system or application controls; and

c. not compromise other systems with which information resources are shared.

Information access restriction

Access to information and application system functions by users and support personnel will be restricted in accordance with the defined access control policy. Restrictions to access will be based on individual business application requirements. The access control policy will also be consistent with the organizational access policy. The following will be implemented in order to support access restriction requirements:

a. providing menus to control access to application system functions;

b. controlling the access rights of users, e.g. read, write, delete, and execute;

c. controlling access rights of other applications; and

d. ensuring that outputs from application systems handling sensitive information contain only the information relevant to the use of the output and are sent only to authorized terminals and locations. This will include periodic reviews of such outputs to ensure that redundant information is removed.

[Implementation – medium term]

Sensitive system isolation

Sensitive systems will have a dedicated (isolated) computing environment. The following points will be implemented for sensitive system isolation:

a. the sensitivity of an application system will be explicitly identified and documented by the application owner; and

b. when a sensitive application is to run in a shared environment, the application systems with which it will share resources and the corresponding risks will be identified and accepted by the owner of the sensitive application.

[Implementation – long term]

Mobile computing and teleworking

To ensure information security when using mobile computing and teleworking facilities, the protection required will be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment will be considered and appropriate protection applied. In the case of teleworking the WCPFC will apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.

Mobile computing and communications

A formal policy will be in place, and appropriate security measures will be adopted to protect against the risks of using mobile computing and communication facilities. When using mobile computing and communicating facilities, e.g. notebooks, palmtops, laptops, smart cards, and mobile phones, special care will be taken to ensure that business information is not compromised. The mobile computing policy will take into account the risks of working with mobile computing equipment in unprotected environments. The mobile computing policy will include the requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection. This policy will also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public places. Protection will be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities. Users of mobile computing facilities in public places will take care to avoid the

risk of overlooking by unauthorized persons. Procedures against malicious software will be in place and be kept up to date.

[Implementation – long term]

Teleworking

A policy, operational plans and procedures will be developed and implemented for teleworking activities. The WCPFC will only authorize teleworking activities if they are satisfied that appropriate security arrangements and controls are in place, and that these comply with the WCPFC's security policy. Suitable protection of the teleworking site will be in place against, e.g., the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the WCPFC's internal systems or misuse of facilities. Teleworking activities will both be authorized and controlled by management, and it will be ensured that suitable arrangements are in place for this way of working. The following matters will be implemented:

a. the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment;

b. the communications security requirements, taking into account the need for remote access to the WCPFC's internal systems, the sensitivity of the information that will be accessed and pass over the communication link and the sensitivity of the internal system;

c. the threat of unauthorized access to information or resources from other persons using the accommodation, e.g. family and friends;

d. the use of home networks and requirements or restrictions on the configuration of wireless network services;

e. policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;

f. access to privately owned equipment (to check the security of the machine or during an investigation), which may be prevented by legislation;

g. software licensing agreements that are such that the WCPFC may become liable for licensing for client software on workstations owned privately by employees, contractors or third party users; and

h. anti-virus protection and firewall requirements.

The guidelines and arrangements to be considered will include:

a. the provision of suitable equipment and storage furniture for the teleworking activities;

b. a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access;

c. the provision of suitable communication equipment, including methods for securing remote access;

d. physical security;

e. rules and guidance on family and visitor access to equipment and information;

f. the provision of hardware and software support and maintenance;

g. the provision of insurance;

h. the procedures for back-up and business continuity;

i. audit and security monitoring; and

j. revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated.

[Implementation – long term]

Information systems acquisition, development and maintenance

Security requirements of information systems

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements will be identified and agreed prior to the development and/or implementation of information systems. All security requirements will be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

Security requirements analysis and specification

Statements of business requirements for new information systems, or enhancements to existing information systems will specify the requirements for security controls. Specifications for the requirements for controls will consider the automated controls to be incorporated in the information system, and the need for supporting manual controls. Similar considerations will be applied when evaluating software packages, developed or purchased, for business applications. Security requirements and controls will reflect the business value of the information assets involved, and the potential business damage, which might result from a failure or absence of security. System requirements for information security and processes for implementing security will be integrated in the early stages of information system projects. If products are purchased, a formal testing and acquisition process will be followed. Contracts with the supplier will address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement then the risk introduced and associated controls will be reconsidered prior to purchasing the product. Where additional functionality is supplied and causes a security risk, this will be disabled or the proposed control structure will be reviewed to determine if advantage can be taken of the enhanced functionality available.

[Implementation – long term]

Correct processing in applications

Appropriate controls will be designed into applications, including user developed applications to ensure correct processing. These controls will include the validation of input data, internal processing and output data. Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls will be determined on the basis of security requirements and risk assessment.

Input data validation

Data input to applications will be validated to ensure that this data is correct and appropriate. Checks will be applied to the input of business transactions, standing data (e.g. names and addresses, credit limits, customer reference numbers), and parameter tables (e.g. sales prices, currency conversion rates, tax rates). The following guidelines will be implemented:

a. dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors:
    i. out-of-range values;
    ii. invalid characters in data fields;
    iii. missing or incomplete data;
    iv. exceeding upper and lower data volume limits;
    v. unauthorized or inconsistent control data;
b. periodic review of the content of key fields or data files to confirm their validity and integrity;
c. inspecting hard-copy input documents for any unauthorized changes (all changes to input documents will be authorized);
d. procedures for responding to validation errors;
e. procedures for testing the plausibility of the input data;
f. defining the responsibilities of all personnel involved in the data input process; and
g. creating a log of the activities involved in the data input process.

[Implementation – medium term]

Control of internal processing

Validation checks will be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. The design and implementation of applications will ensure that the risks of processing failures leading to a loss of integrity are minimized. Specific areas to consider include:

a. the use of add, modify, and delete functions to implement changes to data;
b. the procedures to prevent programs running in the wrong order or running after failure of prior processing;
c. the use of appropriate programs to recover from failures to ensure the correct processing of data; and
d. protection against attacks using buffer overruns/overflows.

An appropriate checklist will be prepared, activities documented, and the results will be kept secure. Examples of checks that can be incorporated include the following:

a. session or batch controls, to reconcile data file balances after transaction updates;
b. balancing controls, to check opening balances against previous closing balances, namely:
    i. run-to-run controls;
    ii. file update totals;
    iii. program-to-program controls;
c. validation of system-generated input data;
d. checks on the integrity, authenticity or any other security feature of data or software downloaded, or uploaded, between central and remote computers;
e. hash totals of records and files;
f. checks to ensure that application programs are run at the correct time;
g. checks to ensure that programs are run in the correct order and terminate in case of a failure, and that further processing is halted until the problem is resolved; and
h. creating a log of the activities involved in the processing.

[Implementation – long term]

Message integrity

Requirements for ensuring authenticity and protecting message integrity in applications will be identified, and appropriate controls identified and implemented. An assessment of security risks will be carried out to determine if message integrity is required and to identify the most appropriate method of implementation.

[Implementation – long term]

Output data validation

Data output from an application will be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Output validation may include:

a. plausibility checks to test whether the output data is reasonable;
b. reconciliation control counts to ensure processing of all data;
c. providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information;
d. procedures for responding to output validation tests;
e. defining the responsibilities of all personnel involved in the data output process;
f. creating a log of activities in the data output validation process.

[Implementation – medium term]

Cryptographic controls

A policy will be developed on the use of cryptographic controls. Key management will be in place to support the use of cryptographic techniques.

Policy on the use of cryptographic controls

A policy on the use of cryptographic controls for protection of information will be developed and implemented and will consider:

a. the management approach towards the use of cryptographic controls across the WCPFC, including the general principles under which business information will be protected;

b. based on a risk assessment, the required level of protection will be identified taking into account the type, strength, and quality of the encryption algorithm required;

c. the use of encryption for protection of sensitive information transported by mobile or removable media, devices or across communication lines;

d. the approach to key management, including methods to deal with the protection of keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;

e. roles and responsibilities, e.g. who is responsible for:

    i. the implementation of the policy;

    ii. the key management, including key generation;

f. the standards to be adopted for the effective implementation throughout the WCPFC; and

g. the impact of using encrypted information on controls that rely upon content inspection (e.g. virus detection).

Cryptographic controls can be used to achieve different security objectives, e.g.:

a. confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;

b. integrity/authenticity: using digital signatures or message authentication codes to protect the authenticity and integrity of stored or transmitted sensitive or critical information; and

c. non-repudiation: using cryptographic techniques to obtain proof of the occurrence or non-occurrence of an event or action.

[Implementation – long term]

Key management

Key management will be in place to support the WCPFC's use of cryptographic techniques. All cryptographic keys will be protected against modification, loss, and

destruction. In addition, secret and private keys will be protection against unauthorized disclosure. Equipment used to generate, store and archive keys will be physically protected. A key management system will be based on an agreed set of standards, procedures, and secure methods for:

a. generating keys for different cryptographic systems and different applications;
b. generating and obtaining public key certificates;
c. distributing keys to intended users, including how keys will be activated when received;
d. storing keys, including how authorized users obtain access to keys;
e. changing or updating keys including rules on when keys will be changed and how this will be done;
f. dealing with compromised keys;
g. revoking keys including how keys will be withdrawn or deactivated;
h. recovering keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information;
i. archiving keys, e.g. for information archived or backed up;
j. destroying keys; and
k. logging and auditing of key management related activities.

In order to reduce the likelihood of compromise, activation, and deactivation dates for keys will be defined so that the keys can only be used for a limited period of time. This period of time will be dependent on the circumstances under which the cryptographic control is being used, and the perceived risk.

[Implementation – long term]

Security of system files

Access to system files and program source code will be controlled, and IT projects and support activities conducted in a secure manner.

Control of operational software

There will be procedures in place to control the installation of software on operational systems. To minimize the risk of corruption to operational systems, the following guidelines will be considered to control changes:

a. the updating of the operational software, applications, and program libraries will only be performed by trained administrators upon appropriate management authorization;
b. operational systems will only hold approved executable code, and not development code or compilers;

c. applications and operating system software will only be implemented after extensive and successful testing; the tests will include tests on usability, security, effects on other systems and user-friendliness, and will be carried out on separate systems; it will be ensured that all corresponding program source libraries have been updated;

d. a configuration control system will be used to keep control of all implemented software as well as the system documentation;

e. a rollback strategy will be in place before changes are implemented;

f. an audit log will be maintained of all updates to operational program libraries;

g. previous versions of application software will be retained as a contingency measure; and

h. old versions of software will be archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data is retained in archive.

Vendor supplied software used in operational systems will be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The WCPFC will consider the risks of relying on unsupported software. Any decision to upgrade to a new release will take into account the business requirements for the change, and the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting this version. Software patches will be applied when they can help to remove or reduce security weaknesses. Physical or logical access will only be given to suppliers for support purposes when necessary, and with management approval. Operating systems will only be upgraded when there is a requirement to do so, for example, if the current version of the operating system no longer supports the business requirements. Upgrades will not take place just because a new version of the operating system is available. New versions of operating systems may be less secure, less stable, and less well understood than current systems.

[Implementation – medium term]

Protection of system test data

Test data will be selected carefully, and protected and controlled. The use of operational databases containing personal information or any other sensitive information for testing purposes will be avoided. If personal or otherwise sensitive information is used for testing purposes, all sensitive details and content will be removed or modified beyond recognition before use. The following guidelines will be applied to protect operational data, when used for testing purposes:

a. the access control procedures, which apply to operational application systems, will also apply to test application systems;

b. there will be separate authorization each time operational information is copied to a test application system;

c. operational information will be erased from a test application system immediately after the testing is complete; and

d. the copying and use of operational information will be logged to provide an audit trail.

[Implementation – long term]

Access control to program source code

Access to program source code will be restricted. Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) will be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries. The following guidelines will then be considered to control access to such program source libraries in order to reduce the potential for corruption of computer programs:

a. where possible, program source libraries will not be held in operational systems;

b. the program source code and the program source libraries will be managed according to established procedures;

c. support personnel will not have unrestricted access to program source libraries;

d. the updating of program source libraries and associated items, and the issuing of program sources to programmers will only be performed after appropriate authorization has been received;

e. program listings will be held in a secure environment;

f. an audit log will be maintained of all accesses to program source libraries; and

g. maintenance and copying of program source libraries will be subject to strict change control procedures.

[Implementation – long term]

Security in development and support processes

Project and support environments will be strictly controlled. Managers responsible for application systems will also be responsible for the security of the project or support environment. They will ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

Change control procedures

The implementation of changes will be controlled by the use of formal change control procedures. Formal change control procedures will be documented and enforced in order to minimize the corruption of information systems. Introduction of new systems and major changes to existing systems will follow a formal process of documentation,

specification, testing, quality control, and managed implementation. This process will include a risk assessment, analysis of the impacts of changes, and specification of security controls needed. This process will also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained. The change procedures will include:

a. maintaining a record of agreed authorization levels;

b. ensuring changes are submitted by authorized users;

c. reviewing controls and integrity procedures to ensure that they will not be compromised by the changes;

d. identifying all software, information, database entities, and hardware that require amendment;

e. obtaining formal approval for detailed proposals before work commences;

f. ensuring authorized users accept changes prior to implementation;

g. ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of;

h. maintaining a version control for all software updates;

i. maintaining an audit trail of all change requests;

j. ensuring that operating documentation and user procedures are changed as necessary to remain appropriate; and

k. ensuring that the implementation of changes takes place at the right time and does not disturb the business processes involved.

[Implementation – long term]

Technical review of applications after operating system changes

When operating systems are changed, business critical applications will be reviewed and tested to ensure there is no adverse impact on organizational operations or security. This process will cover:

a. review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;

b. ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes;

c. ensuring that notification of operating system changes is provided in time to allow appropriate tests and reviews to take place before implementation; and

d. ensuring that appropriate changes are made to the business continuity plans.

A specific group or individual will be given responsibility for monitoring vulnerabilities and vendors' releases of patches and fixes.

[Implementation – medium term]

Restrictions on changes to software packages

Modifications to software packages will be discouraged, limited to necessary changes, and all changes will be strictly controlled. As far as possible, and practicable, vendor-supplied software packages will be used without modification. Where a software package needs to be modified the following points will be considered:

a. the risk of built-in controls and integrity processes being compromised;

b. whether the consent of the vendor will be obtained;

c. the possibility of obtaining the required changes from the vendor as standard program updates; and

d. the impact if the WCPFC becomes responsible for the future maintenance of the software as a result of changes.

If changes are necessary the original software will be retained and the changes applied to a clearly identified copy. A software update management process will be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software. All changes will be fully tested and documented, so that they can be reapplied if necessary to future software upgrades.

[Implementation – long term]

Information leakage

Opportunities for information leakage will be prevented. The following will be considered to limit the risk of information leakage, e.g. through the use and exploitation of covert channels:

a. scanning of outbound media and communications for hidden information;

b. masking and modulating system and communications behaviour to reduce the likelihood of a third party being able to deduce information from such behaviour;

c. making use of systems and software that are considered to be of high integrity, e.g. using evaluated products;

d. regular monitoring of personnel and system activities, where permitted under existing legislation or regulation; and

e. monitoring resource usage in computer systems.

[Implementation – long term]

Outsourced software development

Outsourced software development will be supervised and monitored by the WCPFC. Where software development is outsourced, the following points will be considered:

a. licensing arrangements, code ownership, and intellectual property rights;

b. certification of the quality and accuracy of the work carried out;

c. escrow arrangements in the event of failure of the third party;

d. rights of access for audit of the quality and accuracy of work done;

e. contractual requirements for quality and security functionality of code; and

f. testing before installation to detect malicious and Trojan code.

[Implementation – long term]

Technical Vulnerability Management

Technical vulnerability management will be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations will include operating systems, and any other applications in use.

Control of technical vulnerabilities

Timely information about technical vulnerabilities of information systems being used will be obtained, the WCPFC's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems), and the person(s) within the WCPFC responsible for the software. Appropriate, timely action will be taken in response to the identification of potential technical vulnerabilities. The following guidance will be followed to establish an effective management process for technical vulnerabilities:

a. the WCPFC will define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required;

b. information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them will be identified for software and other technology (based on the asset inventory list). These information resources will be updated based on changes in the inventory, or when other new or useful resources are found;

c. a timeline will be defined to react to notifications of potentially relevant technical vulnerabilities;

d. once a potential technical vulnerability has been identified, the WCPFC will identify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems and/or applying other controls;

e. depending on how urgently a technical vulnerability needs to be addressed, the action taken will be carried out according to the controls related to change management or by following information security incident response procedures;

f. if a patch is available, the risks associated with installing the patch will be assessed (the risks posed by the vulnerability will be compared with the risk of installing the patch);

g. patches will be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated. If no patch is available, other controls will be considered, such as:

    i. turning off services or capabilities related to the vulnerability;

    ii. adapting or adding access controls, e.g. firewalls, at network borders;

    iii. increased monitoring to detect or prevent actual attacks;

    iv. raising awareness of the vulnerability;

h. an audit log will be kept for all procedures undertaken;

i. the technical vulnerability management process will be regularly monitored and evaluated in order to ensure its effectiveness and efficiency; and

j. systems at high risk will be addressed first.

[Implementation – medium term]

Information security incident management

Reporting information security events and weaknesses

Formal event reporting and escalation procedures will be in place. All users will be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of WCPFC assets. They will be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

Reporting information security events

Information security events will be reported through appropriate management channels as quickly as possible. A formal information security event reporting procedure will be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event. A point of contact will be established for the reporting of information security events. It will be ensured that this point of contact is known throughout the WCPFC, is always available and is able to provide adequate and timely response. All users will be made aware of their responsibility to report any information security events as quickly as possible. They will also be aware of the procedure for reporting information security events and the point of contact. The reporting procedures will include:

a. suitable feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed;

b. information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary actions in case of an information security event;

c. the correct behaviour to be undertaken in case of an information security event, i.e.

    i. noting all important details (e.g. type of non-compliance or breach, occurring malfunction, messages on the screen, strange behaviour) immediately;

    ii. not carrying out any own action, but immediately reporting to the point of contact;

d. reference to an established formal disciplinary process for dealing with users who commit security breaches.

Examples of information security events and incidents are:

a. loss of service, equipment or facilities,

b. system malfunctions or overloads,

c. human errors,
d. non-compliances with policies or guidelines,
e. breaches of physical security arrangements,
f. uncontrolled system changes,
g. malfunctions of software or hardware, and
h. access violations.

[Implementation – medium term]

Reporting security weaknesses

All users of information systems and services will be required to note and report any observed or suspected security weaknesses in systems or services. All users will report these matters either to their management or directly to their service provider as quickly as possible in order to prevent information security incidents. The reporting mechanism will be as easy, accessible, and available as possible. They will be informed that they will not, in any circumstances, attempt to prove a suspected weakness.

[Implementation – short term]

Management of information security incidents and improvements

Responsibilities and procedures will be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement will be applied to the response to, monitoring, evaluating, and overall management of information security incidents. Where evidence is required, it will be collected to ensure compliance with legal requirements.

Responsibilities and procedures

Management responsibilities and procedures will be established to ensure a quick, effective, and orderly response to information security incidents. In addition to reporting of information security events and weaknesses, the monitoring of systems, alerts, and vulnerabilities will be used to detect information security incidents. The following guidelines for information security incident management procedures will be considered:

a. procedures will be established to handle different types of information security incident, including:
    i. information system failures and loss of service;
    ii. malicious code;
    iii. denial of service;
    iv. errors resulting from incomplete or inaccurate business data;
    v. breaches of confidentiality and integrity;

vi. misuse of information systems;

b. in addition to normal contingency plans, the procedures will also cover:

   i. analysis and identification of the cause of the incident;

   ii. containment;

   iii. planning and implementation of corrective action to prevent recurrence, if necessary;

   iv. communication with those affected by or involved with recovery from the incident;

   v. reporting the action to the appropriate authority;

c. audit trails and similar evidence will be collected and secured, as appropriate, for:

   i. internal problem analysis;

   ii. use as forensic evidence in relation to a potential breach of contract or regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation;

   iii. negotiating for compensation from software and service suppliers;

d. action to recover from security breaches and correct system failures will be carefully and formally controlled; the procedures will ensure that:

   i. only clearly identified and authorized personnel are allowed access to live systems and data;

   ii. all emergency actions taken are documented in detail;

   iii. emergency action is reported to management and reviewed in an orderly manner;

   iv. the integrity of business systems and controls is confirmed with minimal delay.

The objectives for information security incident management will be agreed with management, and it will be ensured that those responsible for information security incident management understand the WCPFC's priorities for handling information security incidents.

[Implementation – long term]

Learning from information security incidents

There will be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored. The information gained from the evaluation of information security incidents will be used to identify recurring or high impact incidents.

[Implementation – long term]

Collection of evidence

Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence will be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Internal procedures will be developed and followed when collecting and presenting evidence for the purposes of disciplinary action handled within the WCPFC. In general, the rules for evidence cover: admissibility of evidence: whether or not the evidence can be used in court; and weight of evidence: the quality and completeness of the evidence.

To achieve admissibility of the evidence, the WCPFC will ensure that their information systems comply with any published standard or code of practice for the production of admissible evidence.

The weight of evidence provided will comply with any applicable requirements. To achieve weight of evidence, the quality and completeness of the controls used to correctly and consistently protect the evidence (i.e. process control evidence) throughout the period that the evidence to be recovered was stored and processed will be demonstrated by a strong evidence trail. In general, such a strong trail can be established under the following conditions:

a. for paper documents: the original is kept securely with a record of the individual who found the document, where the document was found, when the document was found and who witnessed the discovery; any investigation will ensure that originals are not tampered with;

b. for information on computer media: mirror images or copies (depending on applicable requirements) of any removable media, information on hard disks or in memory will be taken to ensure availability; the log of all actions during the copying process will be kept and the process will be witnessed; the original media and the log (if this is not possible, at least one mirror image or copy) will be kept securely and untouched.

Any forensics work will only be performed on copies of the evidential material. The integrity of all evidential material will be protected. Copying of evidential material will be supervised by trustworthy personnel and information on when and where the copying process was executed, who performed the copying activities and which tools and programs have been utilized will be logged.

[Implementation – long term]

Business continuity management

Information security aspects of business continuity management

A business continuity management process will be implemented to minimize the impact on the WCPFC and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process will identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

The consequences of disasters, security failures, loss of service, and service availability will be subject to a business impact analysis. Business continuity plans will be developed and implemented to ensure timely resumption of essential operations. Information security will be an integral part of the overall business continuity process, and other management processes within the WCPFC. Business continuity management will include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

Including information security in the business continuity management process

A managed process will be developed and maintained for business continuity throughout the WCPFC that addresses the information security requirements needed for the WCPFC's business continuity. The process will bring together the following key elements of business continuity management:

a. understanding the risks the WCPFC is facing in terms of likelihood and impact in time, including an identification and prioritisation of critical business processes;

b. identifying all the assets involved in critical business processes;

c. understanding the impact which interruptions caused by information security incidents are likely to have on the business (it is important that solutions are found that will handle incidents causing smaller impact, as well as serious incidents that could threaten the viability of the WCPFC), and establishing the business objectives of information processing facilities;

d. considering the purchase of suitable insurance which may form part of the overall business continuity process, as well as being part of operational risk management;

e. identifying and considering the implementation of additional preventive and mitigating controls;

f. identifying sufficient financial, organizational, technical, and environmental resources to address the identified information security requirements;

g. ensuring the safety of personnel and the protection of information processing facilities and WCPFC property;

h. formulating and documenting business continuity plans addressing information security requirements in line with the agreed business continuity strategy;

i. regular testing and updating of the plans and processes put in place;

j. ensuring that the management of business continuity is incorporated in the WCPFC's processes and structure; responsibility for the business continuity management process will be assigned at an appropriate level within the WCPFC.

[Implementation – long term]

Business continuity and risk assessment

Events that can cause interruptions to business processes will be identified, along with the probability and impact of such interruptions and their consequences for information security. Information security aspects of business continuity will be based on identifying events (or sequence of events) that can cause interruptions to the WCPFC business processes, e.g. equipment failure, human errors, theft, fire, natural disasters and acts of terrorism. This will be followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period. Business continuity risk assessments will be carried out with full involvement from owners of business resources and processes. This assessment will consider all business processes and will not be limited to the information processing facilities, but will include the results specific to information security. The assessment will identify, quantify, and prioritise risks against criteria and objectives relevant to the WCPFC, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities. Depending on the results of the risk assessment, a business continuity strategy will be developed to determine the overall approach to business continuity. Once this strategy has been created, endorsement will be provided by management, and a plan created and endorsed to implement this strategy.

[Implementation – long term]

Developing and implementing continuity plans including information security

Plans will be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

[Implementation – long term]

Business continuity planning framework

A single framework of business continuity plans will be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. Each business continuity plan will describe the approach for continuity, for example the approach to ensure information or information

system availability and security. Each plan will also specify the escalation plan and the conditions for its activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, any existing emergency procedures, e.g. evacuation plans or fallback arrangements, will be amended as appropriate.

[Implementation – long term]

Testing, maintaining and re-assessing business continuity plans

Business continuity plans will be tested and updated regularly to ensure that they are up to date and effective. Business continuity plan tests will ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked. The test schedule for business continuity plan(s) will indicate how and when each element of the plan will be tested. Each element of the plan(s) will be tested frequently. A variety of techniques will be used in order to provide assurance that the plan(s) will operate in real life. These will include:

a. table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions);

b. simulations (particularly for training people in their post-incident/crisis management roles);

c. technical recovery testing (ensuring information systems can be restored effectively);

d. testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site);

e. tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment); and

f. complete rehearsals (testing that the personnel, equipment, facilities, and processes can cope with interruptions).

[Implementation – long term]

Compliance

Compliance with legal requirements

The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements. Advice on specific legal requirements will be sought from the WCPFC's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow).

Identification of applicable legislation

All relevant statutory, regulatory, and contractual requirements and the WCPFC's approach to meet these requirements will be explicitly defined, documented, and kept up to date for each information system and the WCPFC. The specific controls and individual responsibilities to meet these requirements will be similarly defined and documented.

[Implementation – long term]

Intellectual property rights (IPR)

Appropriate procedures will be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. The following guidelines will be considered to protect any material that may be considered intellectual property:

a. publishing an intellectual property rights compliance policy which defines the legal use of software and information products;

b. acquiring software only through known and reputable sources, to ensure that copyright is not violated;

c. maintaining awareness of policies to protect intellectual property rights, and giving notice of the intent to take disciplinary action against personnel breaching them;

d. maintaining appropriate asset registers, and identifying all assets with requirements to protect intellectual property rights;

e. maintaining proof and evidence of ownership of licenses, master disks, manuals, etc;

f. implementing controls to ensure that any maximum number of users permitted is not exceeded;

g. carrying out checks that only authorized software and licensed products are installed;

h. providing a policy for maintaining appropriate licence conditions;

i. providing a policy for disposing or transferring software to others;

j. using appropriate audit tools;

k. complying with terms and conditions for software and information obtained from public networks;

l. not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law; and

m. not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.

[Implementation – long term]

Protection of organizational records

Important records will be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. Records will be categorized into record types, e.g. accounting records, database records, transaction logs, audit logs, and operational procedures, each with details of retention periods and type of storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keying material and programs associated with encrypted archives or digital signatures, will also be stored to enable decryption of the records for the length of time the records are retained. Consideration will be given to the possibility of deterioration of media used for storage of records. Storage and handling procedures will be implemented in accordance with manufacturer's recommendations. For long term storage, the use of paper and microfiche will be considered. Where electronic storage media are chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period will be included, to safeguard against loss due to future technology change. Data storage systems will be chosen such that required data can be retrieved in an acceptable timeframe and format, depending on the requirements to be fulfilled. The system of storage and handling will ensure clear identification of records and of their retention period as defined by national or regional legislation or regulations, if applicable. This system will permit appropriate destruction of records after that period if they are not needed by the WCPFC. To meet these record safeguarding objectives, the following steps will be taken within the WCPFC:

a. guidelines will be issued on the retention, storage, handling, and disposal of records and information;

b. a retention schedule will be drawn up identifying records and the period of time for which they will be retained;

c. an inventory of sources of key information will be maintained; and

d. appropriate controls will be implemented to protect records and information from loss, destruction, and falsification.

[Implementation – long term]

Data protection and privacy of personal information

Data protection and privacy will be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. The WCPFC data protection and privacy policy will be developed and implemented. This policy will be communicated to all persons involved in the processing of personal information. Compliance with this policy and all relevant data protection legislation and regulations requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a data protection officer, who will provide guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that will be followed. Responsibility for handling personal information and ensuring awareness of the data protection principles will be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personal information will be implemented.

[Implementation – long term]

Prevention of misuse of information processing facilities

Users will be deterred from using information processing facilities for unauthorized purposes. Management will approve the use of information processing facilities. Any use of these facilities for non-business purposes without management approval (see 6.1.4), or for any unauthorized purposes, will be regarded as improper use of the facilities. If any unauthorized activity is identified by monitoring or other means, this activity will be brought to the attention of the individual manager concerned for consideration of appropriate disciplinary and/or legal action. Legal advice will be taken before implementing monitoring procedures. All users will be aware of the precise scope of their permitted access and of the monitoring in place to detect unauthorized use. This can be achieved by giving users written authorization, a copy of which will be signed by the user and securely retained by the WCPFC. Employees of the WCPFC, contractors, and third party users will be advised that no access will be permitted except that which is authorized.

At log-on, a warning message will be presented to indicate that the information processing facility being entered is owned by the WCPFC and that unauthorized access is not permitted. The user has to acknowledge and react appropriately to the message on the screen to continue with the log-on process.

[Implementation – long term]

Regulation of cryptographic controls

Cryptographic controls will be used in compliance with all relevant agreements, laws, and regulations. The following items will be considered for compliance with the relevant agreements, laws, and regulations:

a. restrictions on import and/or export of computer hardware and software for performing cryptographic functions;

b. restrictions on import and/or export of computer hardware and software which is designed to have cryptographic functions added to it;

c. restrictions on the usage of encryption;

d. mandatory or discretionary methods of access by the countries' authorities to information encrypted by hardware or software to provide confidentiality of content.

Legal advice will be sought to ensure compliance with national laws and regulations. Before encrypted information or cryptographic controls are moved to another country, legal advice will also be taken.

[Implementation – long term]

Compliance with security policies and standards, and technical compliance

The security of information systems will be regularly reviewed. Such reviews will be performed against the appropriate security policies and the technical platforms and information systems will be audited for compliance with applicable security implementation standards and documented security controls.

Compliance with security policies and standards

Managers will ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. Managers will regularly review the compliance of information processing within their area of responsibility with the appropriate security policies, standards, and any other security requirements. If any non-compliance is found as a result of the review, managers will:

a. determine the causes of the non-compliance;

b. evaluate the need for actions to ensure that non-compliance do not recur;

c. determine and implement appropriate corrective action; and

d. review the corrective action taken.

Results of reviews and corrective actions carried out by managers will be recorded and these records will be maintained. Managers will report the results to the persons carrying out the independent reviews, when the independent review takes place in the area of their responsibility.

[Implementation – short term]

Technical compliance checking

Information systems will be regularly checked for compliance with security implementation standards. Technical compliance checking will be performed either manually (supported by appropriate software tools, if necessary) by an experienced

system engineer, and/or with the assistance of automated tools, which generate a technical report for subsequent interpretation by a technical specialist. Any technical compliance check will only be carried out by competent, authorized persons, or under the supervision of such persons.

[Implementation – long term]

Information systems audit considerations

There will be controls to safeguard operational systems and audit tools during information systems audits. Protection is also required to safeguard the integrity and prevent misuse of audit tools.

Information systems audit controls

Audit requirements and activities involving checks on operational systems will be carefully planned and agreed to minimize the risk of disruptions to business processes. The following guidelines will be observed:

a. audit requirements will be agreed with appropriate management;

b. the scope of the checks will be agreed and controlled;

c. the checks will be limited to read-only access to software and data;

d. access other than read-only will only be allowed for isolated copies of system files, which will be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;

e. resources for performing the checks will be explicitly identified and made available;

f. requirements for special or additional processing will be identified and agreed;

g. all access will be monitored and logged to produce a reference trail; the use of time-stamped reference trails will be considered for critical data or systems;

h. all procedures, requirements, and responsibilities will be documented; and

i. the person(s) carrying out the audit will be independent of the activities audited.

[Implementation – medium term]

Protection of information systems audit tools

Access to information systems audit tools will be protected to prevent any possible misuse or compromise. Information systems audit tools, e.g. software or data files, will be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.

[Implementation – medium term]