Republic of Zambia

Office of the President
Electronic Government Division

PUBLIC SERVICE INFORMATION COMMUNICATION TECHNOLOGY STANDARDS

Information Security Standard

1st Edition2019

© E-Government Division 2019

Foreword

The e-Government Division has the mandate of formulating and enforcing Standards in Information and Communication Technology (ICT) across all Ministries, Provinces and Spending Agencies (MPSAs) to facilitate the transition into a Digital Society. In view of this mandate, the e-Government Division has developed the Public Service ICT Information Security Standard to ensure adherence and compliance by all MPSAs to approved security standards.

The Information Security Standard is intended to facilitate seamless security of data/information between various existing Government Information Systems and Applications owned by different Public Service institutions. MPSAs must ensure that Information Systems and Applications in the Public Service are compliant to set standards in order to be integrated into the Government Information Infrastructure.

The implementation of this standard will be monitored by the National ICT Standards Review Committee while the e-Government Division will undertake enforcement. Annual audits shall be carried out in all the MPSAs to determine their compliance to this standard. The Division will issue a certificate of compliance to an MPSA upon completion of a successful audit assessment. For non-compliant MPSAs, a report detailing the extent of the deviation and the prevailing circumstances shall be tabled before the National ICT Standards Review Committee who will advise on the appropriate action to be taken.

All MPSAs are required to ensure full compliance to this standard for effective and efficient service delivery.

Martine G. Mtonga (Dr)
National Coordinator
SMART ZAMBIA INSTITUTE

Acknowledgement

The development of the Public Service ICT Information Security Standard marks an achievement of a key milestone towards cost effective and efficient implementation of ICT information security in the public service. The standard will assist Government to ensure a coordinated and collaborative approach to implementation of several initiatives under the e-Government programme.

It is for this reason that I wish to commend the e-Government Standards Task Team, Heads of ICT in Ministries, Provinces and other Spending Agencies (MPSAs) and various stakeholders for their unwavering efforts in the development of the ICT information security standard. The document will ensure that ICT standards are implemented in an effective and standardized manner.

Percive Chinyama
Director - Standards
SMART ZAMBIA INSTITUTE

Abbreviations and Acronyms

CMS	Content Management System
ICT	Information & Communications Technology
HTML	Hyper Text Markup Language
MPSA	Ministry, Province and Spending Agency
SLA	Service Level Agreement
SMART	Sustainable, Modern, Achievable, Real-Time
SZI	SMART Zambia Institute
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAFs	Web Application Firewalls
XHTML	Extensible Hyper Text Markup Language
XML	Extensible Markup Language

Document Information

File Name	**Public Service Information Security Standards**
Document Description	Provides compliance requirements for Standards Governing ICT Information Security in Government
Original Authors	ICT Standards Technical Task Team
Creation Date	August, 2018
Last Update	February, 2019
Report Number	1
Version	Version 1.0 (F)

Document Approval

Standards Review Committee Members	**Title**	**Signature**	**Date**
Dr. Martine G. Mtonga	National Coordinator		
Mr. Percive Chinyama	Director - Standards		

Document Distribution

Name	**Title**	**Organisation**
Dr. Martine G. Mtonga	National Coordinator	SMART Zambia
Mr. Percive Chinyama	Director - Standards	SMART Zambia
Mr. Milner Makuni	Director – eGovernment	SMART Zambia
Stakeholders	Directors and Managers	ZABS, MCT and ZICTA All
Heads of ICT	Heads of ICT	All MPSAs

Document History/Record of Updates

Date	**Author/s**	**Version**	**Description**
August, 2018	ICT Standards Technical Task Team	Issue 1.0 (W)	Produced by The Division
October, 2018	ICT Standards Technical Task Team	Issue 1.0 (D)	Produced by The Division
February, 2019	The Division Management	Issue 1.0 (F)	Produced by The Division

Table of Contents

CHAPTER 1

1.0 INTRODUCTION

The Information Security Standard aims at guiding the setting up of appropriate controls that will ensure the protection of information from a wide range of threats in order to ensure continuity in government operations, minimise risk, and maximise return on government ICT investments.

This document provides guidelines for the implementation of suitable controls, including processes, procedures, organisational structures, and software and hardware functions to ensure that information security is achieved. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific ICT security and operational objectives of the Government are met.

This document specifies information security standards for Government Ministries, Provinces and Spending Agencies (MPSAs).

Information security is based on the following elements:

a) Confidentiality – ensuring that information is only accessible to those with authorised access;

b) Integrity – safeguarding the accuracy and completeness of information and processing methods;

c) Availability – ensuring that authorised Users have access to information when required;

d) Compliant use – Ensuring that MPSAs meet all legal and contractual obligation; and.

e) Responsible use – ensuring that appropriate controls are in place so that users of government ICT resources do not adversely affect other users or other systems.

2.0. SCOPE

This document provides for information security standards for MPSAs.

3.0. OBJECTIVE

The objective of the Information Security Standards is to ensure a secure environment for ICTs and enhance user confidence and trust.

4.0. SUB-DOMAINS

The following are the sub domains covered in this document:

1. Information Security Guidelines;
2. Organising Information Security;

3. Asset Management;
4. Human Resources Security;
5. Physical and Environmental Security;
6. Communications Security;
7. Cryptography Controls;
8. Operations Security;
9. Access Control;
10. Information Systems Acquisition, Development and Maintenance;
11. Information Security Incident Management;
12. Supplier Relationships; and
13. Business Continuity Management.

5.0 COMPLIANCE

5.1 Information Security Standards

5.1.1 Guidelines for Information Security

5.1.1.1 Guidance

a) MPSAs shall develop an "Information Security Guideline" which is approved by management and which sets out the institution's approach to managing its information security objectives.

b) These guidelines shall be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, e.g. in the context of an "information security awareness, education and training programme".

c) The guidelines shall address regulations, legislation and contracts;

5.1.1.2 Structure

The ICT guideline shall contain: -

a) Definition of information security, objectives and principles to guide all activities relating to ICT information security within an Institution;

b) Assignment of general and specific responsibilities for information security management to the MPSA Information Security Working Group to have defined roles;

c) Processes for handling deviations and exceptions.

5.1.2 Review of the guidelines for information security

5.1.2.1 Guidance

a. The guidelines for information security shall be reviewed every after 2 years or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

b. The review shall include assessing opportunities for improvement of the organisation's guidelines and approach to managing information security in response to changes to the organisational environment, operational circumstances, legal conditions or technical environment.

c. The review of guidelines for information security shall take the results of management reviews into account.

5.1.2.2 Approval of Guidelines

The National ICT Standards Review committee shall approve the revised guidelines obtained from the MPSA Information Security Working Group.

5.2 Organisation of Information Security

5.2.1 Internal Organisation

5.2.1.1 Information Security Roles and Responsibilities

The Information security roles and responsibilities are as outlined below:

a. MPSAs shall have an Information Security Steering Committee.

b. Senior Management Agenda/Minutes shall include information security matters.

c. MPSAs shall designate one or more officers in charge of information security.

d. To be able to fulfil responsibilities in the information security area the appointed individuals shall be certified in the area and given opportunities to keep up to date with developments in the information security sector.

e. Information security roles and responsibilities shall be documented and approved by Senior Management in the MPSAs.

f. Employees with information security roles and responsibilities shall sign a consent document stating that they understand their roles and responsibilities.

5.2.1.2 Segregation of Duties

a. MPSAs shall ensure that no single person can access, modify or use assets without authorization or detection. The initiation of an event shall be separated from its authorization. The possibility of collusion shall be considered in designing the controls.

b. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision shall be considered.

5.2.1.3 Emergency Response

a. MPSAs shall contact the Public Service Computer Emergency Response Team (CERT) to report cyber space attacks for action to be taken.

b. MPSAs shall have contacts with other authorities including utilities, emergency services, telecommunication providers, electricity suppliers and health and safety.

5.2.1.4 Contact with Special Interest Groups

a. MPSAs ICT security personnel shall maintain membership with specialist security forums and professional associations.

5.2.1.5 Information Security in Project Management

a. Information security objectives shall be included in all projects’ objectives;

b. An information security risk assessment shall be conducted at an early stage of the project to identify necessary controls; and

c. Information security shall be part of all phases of the applied project management methodology.

5.3 Asset Management

5.3.1 Responsibility for Assets

a. Inventory of assets

i. MPSAs shall implement and maintain an inventory of assets associated with information and information processing facilities.

ii. The asset inventory shall be accurate, up to date, consistent and aligned with other inventories.

iii. For each of the identified assets, ownership of the asset shall be assigned, and the classification shall be identified.

b. Ownership of Assets

i. MPSAs shall assign each information asset to an owner.

ii. The assigned owner shall ensure that assets are inventoried, appropriately classified, protected and ensure proper handling and disposal if and when the asset is destroyed.

5.3.2 Information Classification

a. Classification of Information

i. Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

ii. The scheme shall also be aligned to the access control guideline.

iii. Each level shall be given a name that makes sense in the context of the classification scheme's application.

iv. The scheme shall be consistent across the whole organisation.

v. Classification shall be included in the organisation's processes and be consistent and coherent across the organisation. Results of classification shall indicate value of assets depending on their sensitivity and criticality to the organisation, e.g. in terms of confidentiality, integrity and availability.

vi. Results of classification shall be updated in accordance with changes of their value, sensitivity and criticality through their lifecycle.

vii. Information confidentiality classification scheme shall be based on four levels as follows:

- Disclosure causes no harm;
- Disclosure causes minor embarrassment or minor operational inconvenience;
- Disclosure has a significant short-term impact on operations or tactical objectives;
- Disclosure has a serious impact on long term strategic objectives or puts the survival of the organisation at risk.

Note that the above listed classification should be in line existing Public Service Security Guidelines.

b. Labelling of Information

MPSAs shall ensure labelling of classified information. Physical labels and metadata shall be used.

5.3.3 Media Handling

a. Management of Removable Media

MPSAs shall develop procedures for the management of removable media in accordance with the classification scheme adopted by the organisation.

b. Disposal of Media

MPSAS shall document formal procedures for the secure disposal of media to minimize the risk of confidential information leakage to unauthorized persons.

c. Physical Media transfer

MPSAs shall document and implement guidelines to protect media containing information being transported:

5.4 Human Resource Security

I. Prior to employment relevant screening and verification checks will be conducted on candidates.

II. Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and if these are handling confidential information, the organisation shall also consider further, more detailed verifications.

III. Screening process shall also be ensured for contractors. In these cases, the agreement between the MPSAs and the contractor shall specify responsibilities for conducting the screening and the notification procedures that need to be followed as well as consequences.

IV. Information on all candidates being considered for positions within the MPSAs shall be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates shall be informed beforehand about the screening activities.

V. During employment MPSAs shall ensure all employees and contractors are properly briefed on their information security roles and responsibilities prior to being granted access to classified information or information systems.

a. Information Security Awareness, Education and Training

MPSAs shall conduct an information security awareness programme in line with the organisation's information security guidelines and relevant procedures.

Information security education and training shall take place annually. Initial education and training applies to those who transfer to new positions or roles with substantially different information security requirements, not just to new recruits and should take place before the role becomes active.

The MPSAs shall develop the education and training programme in order to conduct the education and training effectively. The programme should be in line with the organisation's information security guidelines and relevant procedures.

b. Disciplinary Process

MPSAs shall have a disciplinary process and take action against employees who have committed an information security breach as per Public Service Terms and Conditions of Employment.

VI. Termination and change of employment

a. Termination or Change of Employment Responsibilities

MPSAs shall ensure that the communication of termination responsibilities include on-going information security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement and the terms and conditions of employment.

Changes of responsibility or employment shall be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment.

MPSAs shall inform employees, customers or contractors of changes to personnel and operating arrangements

5.5 Physical and Environmental Security

5.5.1 Secure Areas

5.5.1.1 Physical Security Perimeter

a. MPSAs shall label security perimeters to protect areas that contain either sensitive or critical information or information processing facilities.

b. The identified security perimeters shall be documented together with their risk assessment.

5.5.1.2 Physical Entry Controls

a. MPSAs shall ensure the reason for authorization, date and time of entry and departure of visitors shall be recorded, and all visitors shall be supervised unless their access has been previously approved; The identity of visitors shall be authenticated by an appropriate means;

b. A physical logbook or electronic audit trail of all access shall be securely maintained and monitored;

c. Externally contracted personnel shall be granted restricted access to secure areas or information processing facilities only when required;

5.5.1.3 Securing Rooms and Facilities

MPSAs shall ensure Key facilities are sited to avoid access by the public and where applicable, buildings shall be unobtrusive and give minimum indication of their purpose.

5.5.1.4 Protecting Against External and Environmental Threats

Specialist advice shall be obtained from the Public Service ICT Standards Technical Committee on how to avoid damage from earthquake, explosion, civil unrest and other forms of natural or man-made disaster.

5.5.1.5 Working in Secure Areas

MPSAs shall consider the following:

i. Personnel shall only be aware of the existence of, or activities within, a secure area on a need to-know basis;

ii. Unsupervised working in secure areas shall be avoided both for safety reasons and to prevent opportunities for malicious activities;

iii. Vacant secure areas shall be physically locked and periodically reviewed;

iv. Photographic, video, audio or other recording equipment, such as cameras in mobile devices, shall not be allowed in secure areas, unless authorized.

v. The arrangements for working in secure areas include controls for the employees and externally contracted workers working in the secure area and they cover all activities taking place in the secure area.

5.5.1.6 Delivery and Loading Areas

MPSAs shall ensure the following;

i. Access to a delivery and loading area from outside of the building shall be restricted to identified and authorized personnel;

ii. The delivery and loading area shall be designed so that supplies can be loaded and unloaded without delivery personnel gaining access to other parts of the building;

iii. The external doors of a delivery and loading area shall be secured when the internal doors are opened;

iv. Incoming material shall be inspected and examined for explosives, chemicals or other hazardous materials, before it is moved from a delivery and loading area;

v. Incoming material shall be registered in accordance with asset management procedures on entry to the site;

vi. Incoming and outgoing shipments shall be physically segregated, where possible; and

vii. Incoming material shall be inspected for evidence of tampering en-route and be immediately reported to security personnel If such tampering is discovered.

5.6 Communications Security

5.6.1 Network Security Management

5.6.1.1 Network Controls

a. MPSAs shall develop and document controls to ensure the security of information in networks and the protection of connected services from unauthorized access.

b. Responsibilities and procedures for the management of networking equipment shall be established;

c. Operational responsibility for networks should be separated from computer operations where appropriate;

d. Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications;

e. special controls may also be required to maintain the availability of the network services and the connected computers;

f. Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security;

g. Management activities should be closely coordinated both to optimize the service to the Organisation and to ensure that controls are consistently applied across the information processing infrastructure; and

h. Systems on the network should be authenticated and system connection to network restricted;

5.6.1.2 Security of Network Services

MPSAs shall develop Service Level Agreements (SLAs) for network services, the SLAs shall define security requirements and the right to audit. (Consider development of Service Charters and parties to SLA).

5.6.1.3 Segregation in Networks

a. MPSAs shall divide large networks into separate network domains based on trust either physically into different networks or by using different logical networks.

b. The perimeter of each domain shall be well defined. Access between network domains shall be allowed but shall be controlled at the perimeter using a gateway (e.g. firewall, filtering router).

c. Wireless networks require special treatment due to the poorly defined network perimeter. For sensitive environments, all wireless access must be treated as external connections and segregated from internal networks until the access has passed through a gateway in accordance with network controls guidelines before granting access to internal systems.

d. The authentication, encryption and user level network access control technologies of modern, standards based wireless networks may be sufficient for direct connection to the organisation’s internal network when properly implemented.

5.6.2 Information Transfer

5.6.2.1 Information Guidelines and Procedures

a. MPSAs shall develop formal transfer guidelines, procedures and controls to protect the transfer of information using all types of communication facilities.

5.6.2.2 Agreements on Information Transfer

a. MPSAs shall have agreements to address the secure transfer of business information between the Organisation and external parties.

b. The information security content of the agreement shall indicate the sensitivity of the business information involved.

5.6.2.3 Electronic Messaging

MPSAs shall develop and implement the following guidelines:

a. Protecting messages from unauthorised access, or denial of service commensurate with the scheme adopted by the organisation;

b. Legal considerations, for example requirements for electronic signatures;

c. Obtaining approval prior to using external public services such as instant messaging, social networking or sharing;

d. Stronger levels of authentication controlling access from publicly accessible networks or non-disclosure agreements;

.

b. Identify, regularly review and document requirements for non-disclosure;

c. Identify, responsibilities and actions of signatories to avoid unauthorised information disclosure;

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

e. Document expected actions to be taken in case of a breach of the agreement; and

f. There shall be forms of non- disclosure agreements in different circumstances.

5.7 Cryptography Controls

5.7.1 Guidelines on the Use of Cryptographic Controls

a. MPSAS shall develop and implement a guideline on the use of cryptographic controls for protection of information.

b. The guidelines shall address the following:

i. Management approach towards the use of cryptographic controls across the Organisation, including the general principles under which business information should be protected;

ii. The required level of protection, considering the type, strength and quality of the encryption algorithm required. This should be based on risk assessment;

iii. The use of encryption for protection of information transported by mobile or removable media devices or across communication lines; and

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

5.7.2 Roles and responsibilities

a. MPSAs shall consult the National Coordinator – e-Government Division to get specialist advice in selecting appropriate cryptographic controls to meet the information security guideline objectives. The e-Government shall develop and implement a guideline on the use, protection and lifetime of cryptographic keys.

b. The key management guideline shall be based on the following:

i. An agreed set of standards, procedures and secure methods for generating keys for different cryptographic systems and different applications;

ii. Issuing, obtaining and storing of keys i.e. distributing and storing of keys;

iii. Changing or updating keys including rules on when keys should be changed and how this will be done;

iv. Dealing with compromised keys;

v. Revoking, Recovering and Destroying of keys including how keys should be withdrawn or deactivated; and

vi. Logging and auditing of key management related activities;

c. In order to reduce the likelihood of improper use, activation and deactivation dates for keys shall ensure that the keys can only be used for the period in the associated key management guideline;

d. In addition to securely managing secret and private keys, the authenticity of public keys shall also be considered. This authentication process can be done using public keys which shall be issued by the Division;

e. The contents of SLAs or contracts with external suppliers of cryptographic services, shall cover issues of liability, reliability of services and response times for the provision of services; and

f. Procedures may need to be considered for handling legal requests for access to cryptographic keys, e.g. encrypted information can be required to be made available in an unencrypted form as evidence in a court case;

5.7.3 Business Requirements of Access Control

5.7.3.1 Access Control Guideline

a. MPSAs shall establish, document and review an access control guideline based on business and information security requirements.

b. The guideline shall take account of the following:

  i. Security requirements of business applications;

  ii. Guidelines for information dissemination and authorization;

  iii. Consistency between the access rights and information guidelines of systems and networks;

  iv. Relevant legislation and any contractual obligations regarding limitation of access to data or services;

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

  vi. Segregation of access control roles;

  vii. Requirements for formal authorization of access requests;

  viii. Requirements for periodic review of access rights;

  ix. Removal of access rights;

x. Archiving of records of all events concerning the use and management of user identities and secret authentication information;

c. Role based access control.

d. The guideline shall be based on a need-to-know and need-to-use;

e. MPSAs shall develop a guideline concerning the use of networks and network services. This guideline shall cover:

i. The networks and network services which can be accessed;

ii. Authorization procedures for determining who can access which networks and networked services;

iii. Management controls and procedures to protect access to network connections and network services;

iv. The means used to access networks and network services;

v. User authentication requirements for accessing various network services;

vi. Monitoring of the use of network services; and

vii. The guideline on the use of network services should be consistent with the organisation’s Access Control Guideline.

5.7.3.2 System and Application Access Control

i. Information Access Restriction

a. MPSAs shall implement restrictions to access based on individual business application requirements and in accordance with the access control guideline.

b. MPSAs shall design a procedure for logging into a system to minimize the opportunity for unauthorised access. The log-on procedure shall disclose the minimum of information about the system or application.

ii. Password Management System

a. The organisation shall establish a password management system.

b. The password management system shall:

i. Enforce the use of individual user IDs and passwords to maintain accountability;

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

iii. Enforce a choice of quality passwords;

iv. Force users to change their passwords at the log-on;

v. Enforce regular password changes as needed;

vi. Maintain a record of previously used passwords and prevent re-use;

vii. Not display passwords on the screen when being entered;

viii. Store password separately from application system data; and

ix. Store and transmit passwords in protected form.

iii. Use of Privileged Utility Programs

a. In case an MPSA is using utility program, the following guidelines shall be considered and documented:

i. Use of authentication and authorization procedures for utility programs;

ii. Segregation of utility programs from applications software;

iii. Limitation of the use of utility programs to the minimum practical number of trusted, authorized users;

iv. Authorization for ad hoc use of utility programs;

v. Limitation of the availability of utility programs, e.g. for the duration of an authorised change;

vi. Logging of all use of utility programs and documenting of authorization levels for utility programs;

vii. Removal or disabling of all unnecessary utility programs;

viii. Not making utility programs available to users who have access to applications on systems where segregation of duties is required.

5.7.3.3 Access Control to Program Source Code

a. MPSAs shall document the following guidelines to control access to program source libraries in order to reduce the potential for corruption of computer programs:

i. Where possible, program source libraries shall not be held in operational systems;

ii. The program source code and the program source libraries shall be managed according to established procedures;

iii. Support personnel should not have unrestricted access to program source libraries;

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

v. Program listings shall be held in a secure environment;

vi. An audit log should be maintained of all accesses to program source libraries; and

vii. Maintenance and copying of program source libraries shall be subject to strict change control procedures.

b. If the program source code is intended to be published, additional controls to help getting assurance on its integrity (e.g. digital signature) should be considered.

5.7.4 Encryption

The e-Government Division and or Systems Development Contractor shall create a standardized procedure for encrypting information which includes the following tasks;

i. Analyse the risks of not using appropriately effective encryption and hashing schemes to protect information among different applications;

ii. Define the minimum encryption and hashing key length / algorithm/function combination that should be used;

iii. Make reference to recommendations provided by the National Technical Committee;

iv. Analyse the requirement of using digital certificates across different applications;

v. Modify the applications to use the new encryption standards; and

vi. The Contractor shall submit the encryption key and architecture to the e-Government Division or it's appointed Agents.

5.8 Operations Security

5.8.1 Operational Procedures and Responsibilities

5.8.1.1 Documented Operating Procedures

a. MPSAs shall document operating procedures and make them available to all users who need them.

b. The operating procedures shall specify the operational instructions, including:

i. The installation and configuration of systems;

ii. Processing and handling of information both automated and manual;

iii. Backup and scheduling requirements, including interdependencies with other systems;

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

v. Support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties;

vi. Special output and media handling instructions;

vii. System restart and recovery procedures for use in the event of system failure;

viii. The management of audit-trails and system log information monitoring procedures;

c. Operating procedures and the documented procedures for system activities shall be treated as formal documents and changes will be authorised by management; and

d. Where technically feasible, information systems shall be managed consistently, using the same procedures, tools and utilities.

5.8.1.2 Change Management

MPSAs shall ensure the following:

Identification and recording of significant changes;

i. Planning and testing of changes;

iii. Assessment of the potential impacts, including information security impacts, of such changes;

ii. Formal approval procedures for proposed changes;

iii. Verification that information security requirements have been met;

iv. Communication of change details to all relevant persons;

vii. Fall-back procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events; and

viii. Provision of an emergency change process to enable quick and controlled.

5.8.1.3 Capacity Management

MPSAs shall ensure:

i. Deletion of obsolete data (storage space);

ii. Decommissioning of applications, systems, databases or environments;

iii. Optimizing batch processes and schedules;

iv. Optimizing application logic or database queries;

v. Denying or restricting bandwidth for resource-hungry services if these are not business critical (e.g. video streaming); and

vi. A documented capacity management plan shall be considered for mission critical systems.

5.8.1.4 Separation of Development, Testing and Operational Environments

The following items shall be documented and implemented:

i. Rules for the transfer of software from development to operational status shall be defined and documented;

ii. Development and operational software shall run on different systems or computer processors and in different domains or directories;

iii. Changes to operational systems and applications shall be tested in a testing or staging environment prior to being applied to operational systems;

iv. Other than in exceptional circumstances, testing shall not be done on operational systems;

v. Compilers, editors and other development tools or system utilities shall not be accessible from operational systems when not required;

vi. Users shall use different user profiles for operational and testing systems, and menus should display appropriate identification messages to reduce the risk of error; and

vii. Sensitive data shall not be copied into the testing system environment unless equivalent controls are provided for the testing the system.

5.8.2 Protection from Malware

MPSAs shall implement controls for detection, prevention and recovery controls to protect against malware combined with appropriate user awareness.

a. The following shall be implemented:

i. Establishing a formal guideline prohibiting the use of unauthorized software;

ii. Implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blacklisting);

iii. Establishing a formal guideline to protect against risks associated with obtaining software either from or via external networks or on any other medium, indicating what protective measures shall be taken;

iv. Reducing vulnerabilities that could be exploited by malware;

iv. Conducting regular reviews of the software and data content of systems supporting critical business Processes;

vii. The presence of any unapproved or unauthorized amendments should be formally investigated;

viii. Installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis;

ix. Procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks;

x. Preparing appropriate business continuity plans for recovering from malware attacks;

xi. Implementing procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware;

xii. Implementing procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative;

xiii. All heads of IT shall ensure that credible sources or suppliers producing software protecting against malware, are used to differentiate between hoaxes and real malware; and

xiv. All users should be made aware of the problem of hoaxes and what to do on receipt of them;

5.8.3 Backup

5.8.3.1 Information Backup

a. The e-Government Division shall define a backup guideline to define the organisation's requirements for backup of information, software and systems.

b. When designing a backup plan, the following items shall be taken into consideration:

i. Accurate and complete records of the backup copies and documented restoration procedures shall be produced;

ii. The extent and frequency of backups shall reflect the business requirements of the organisation;

iii. The backups shall be stored in a remote location, with enough distance away from the system site to escape any damage from a disaster at the main site;

iv. Backup information shall be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site;

v. Backup media shall be regularly tested to ensure that they can be relied upon for emergency use when necessary. This shall be combined with a test of the restoration procedures and checked against the restoration time required.

vi. In situations where confidentiality is of importance, backups shall be protected by means of encryption.

vii. Operational procedures shall monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the backup guideline.

viii. Backup arrangements for individual systems and services shall be regularly tested to ensure that they meet the requirements of business continuity plans.

ix. In the case of critical systems and services, backup arrangements should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

x. The retention period for essential business information shall be determined, taking into account any requirement for archive copies to be permanently.

5.8.4 Logging and Monitoring

5.8.4.1 Event Logging

a. Electronic event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed by MPSAs.

b. Event logs shall include:

   i. user IDs;

ii. System activities;

iii. Dates, times and details of key events, e.g. log-on and log-off;

iv. Device identity or location if possible and system records of successful and rejected system access attempts;

v. Records of successful and rejected data and other resource access attempts;

vi. Changes to system use of privileges;

vii. Use of system utilities and applications;

viii. Files accessed and the kind of access;

ix. Network addresses and protocols;

x. Alarms raised by the access control system;

xi. Activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems; and

xii. Records of transactions executed by users in applications.

c. Event logs can contain sensitive data and personal information.

d. Appropriate privacy protection measures shall be taken.

e. System Administrators shall not have permission to erase or de-activate logs of their own activities.

5.8.4.2 Protection of Log Information

a. Logging facilities and log information shall be protected against tampering and unauthorized access.

b. Controls shall aim to protect against unauthorized changes to log information and operational problems with the logging facility.

5.8.4.3 Administrator and Operator Logs

a. System administrator and system operator activities shall be logged as well as the logs protected and regularly reviewed.

5.8.4.4 Clock Synchronization

a. External and internal requirements for time representation, synchronization and accuracy shall be documented.

b. A standard reference time for use within the organisation shall be identified, documented and implemented.

c. The organisation's approach to obtaining a reference time from external source(s) and how to synchronize internal clocks reliably shall be documented and implemented.

5.8.5 Control of Operational Software

5.8.5.1 Installation of software on Operational Systems

a. MPSAs shall document procedures to control changes of software on operational systems.

b. The procedures shall include:

i.The updating of the operational software, applications and program

ii. Libraries shall only be performed by trained administrators upon

appropriate management authorization;

iii. Operational systems shall only hold approved executable code;

iv. Applications and operating system software shall only be implemented after successful testing;

v. It shall be ensured that all corresponding program source libraries have been updated;

vi. A control system shall be used to keep control of all;

vii. A rollback strategy shall be in place before changes are implemented;

viii. An audit log shall be maintained of all updates to operational program libraries;

ix. Previous versions of application software shall be retained as a contingency measure; and

x. Old versions of software shall be archived, together with all required information, activation keys, parameters, procedures, details and supporting software for as long as the data are retained.

c. Vendor supplied software used in operational systems shall be maintained at a level supported by the supplier.

d. Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release.

e. Software patches shall be applied when they can help to remove or reduce information security weaknesses.

f. Physical or logical access shall only be given to suppliers for support purposes when necessary and with management approval. The supplier's activities shall be monitored.

g. Computer software may rely on externally supplied software and modules, which shall be monitored and controlled to avoid unauthorized changes, which could introduce security weaknesses.

5.8.6 Technical Vulnerability Management

5.8.6.1 Management of Technical Vulnerabilities

i. MPSAs shall develop and maintain an effective management process for technical vulnerabilities

ii. The process shall contain:

  i. Roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required;

  ii. Information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them shall be identified for software and other technology;

iii. These information resources shall be updated based on changes in the inventory or when other new or useful resources are found;

iv. A timeline shall be defined to react to notifications of potentially relevant technical vulnerabilities;

v. Once a potential technical vulnerability has been identified, the organisation should identify the associated risks and the actions to be taken;

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

vii. If a patch is available from a legitimate source, the risks associated with installing the patch shall be assessed;

viii. Patches shall be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated;

iii. An audit log should be kept for all procedures undertaken;

iv. The technical vulnerability management process shall be regularly monitored and evaluated in order to ensure its effectiveness and efficiency;

v. Systems at high risk should be addressed first;

vi. An effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur; and

vii. Define a procedure to address the situation where vulnerability has been identified but there is no suitable counter measure.

5.8.6.2 Restrictions on Software Installation

a. The eGovernment Division or an authorised MPSA shall define and enforce strict guidelines on which types of software users may install.

b. The guideline of least privilege shall be applied. If granted certain privileges, users may have the ability to install software. The eGovernment Division and authorised MPSA shall identify and document what types of software installations are permitted.

These privileges shall be granted having regard to the roles of the users concerned.

5.8.6.3 Information Systems Audit Considerations

MPSAs shall document and observe the following:

i. Audit requirements for access to systems and data shall be agreed with appropriate management;

ii. The scope of technical audit tests shall be agreed and controlled;

iii. Audit tests shall be limited to read-only access to software and data;

iv. Access other than read-only shall only be allowed for isolated copies of system files, which shall be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;

v. Requirements for special or additional processing shall be identified and agreed upon;

vi. Audit tests that could affect system availability shall be run outside business hours or off-peak period as determined by set guidelines; and

vii. All access shall be monitored and logged to produce a reference trail.

5.9 Access Control

Business requirements of access control can be considered as outlined below.

5.9.1 Access Control Guideline

a. MPSAs shall establish, document and review an access control guideline based on business and information security requirements.

b. The guideline shall take account of the following:

i. Security requirements of business applications;

ii. Guidelines for information dissemination and authorization:

a. Consistency between the access rights and information guidelines of systems and networks;

b. Relevant legislation and any contractual obligations regarding limitation of access to data or services;

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

d. Segregation of access control roles, e.g. access request, access authorization, access administration; and

e. Requirements for formal authorization of access requests;

iii. Role based access control is an approach used successfully by many organizations to link access rights with business roles.

a. The guideline shall be based on need-to-know and need-to-use basis Access to networks and network services.

b. MPSAs shall develop a guideline concerning the use of networks and network services.

c. This guideline shall cover:

i. The networks and network services which are authorised to be accessed;

ii. Authorization procedures for determining who can access which networks and networked services;

iii. Management controls and procedures to protect access to network connections and network services;

iv. The means used to access networks and network services (e.g. use of VPN or wireless network);

v. User authentication requirements for accessing various network services;

vi. Monitoring of the use of network services; and

vii. The guideline on the use of network services should be consistent with the organisation's Access Control Guideline.

5.9.3 User Access Management

5.9.3.1 User Registration and De-registration

a. MPSAs shall develop a formal user registration and de-registration process to enable assignment of access rights.

b. The process for managing user IDs should include:

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

ii. The use of shared IDs should only be permitted where they are necessary for business or operational reasons and should be approved and documented;

iii. Immediately disabling or removing user IDs of users who have left the organisation;

iv. Periodically identifying and removing or disabling redundant user IDs; and

v. Ensuring that redundant user IDs are not issued to other users.

5.9.3.2 User Access Provisioning

a. MPSAs shall develop and implement a formal user access provisioning process to assign or revoke access rights for all user types to all systems and services.

b. The provisioning process for assigning or revoking access rights granted to user IDs shall include:

i. Obtaining authorization from the owner of the information system or service for the use of the information system or service;

ii. Separate approval for access rights from management may also be appropriate;

iii. Verifying that the level of access granted is appropriate to the access guidelines and is consistent with other requirements such as segregation of duties;

iv. Ensuring that access rights are not activated (e.g. by service providers) before authorization procedures are completed;

v. Maintaining a central record of access rights granted to a user ID to access information systems and services;

vi. Adapting access rights of users who have changed roles or jobs and immediately removing or blocking access rights of users who have left the organisation; and

vii. Periodically reviewing access rights with owners of the information systems or services.

5.9.4 Management of Privileged Access Rights

MPSAS shall ensure the allocation of privileged access rights is controlled through a formal authorization process in accordance with the relevant access control guidelines. The following steps shall be considered:

i. The privileged access rights associated with each system or process, e.g. operating system, database management system and each application and the users to whom they need to be allocated should be privileged access rights. These rights shall be allocated to users on a need-to-use basis and on an event by event basis in line with the access control guidelines, i.e. based on the minimum requirement for their functional roles;

ii. An authorization process and a record of all privileges allocated should be maintained. Privileged access rights shall not be granted until the authorization process is complete;

iii. Requirements for expiry of privileged access rights shall be assigned to a user ID different from those used for regular business activities. Regular business activities shall not be performed from privileged IDs;

iv. The competencies of users with privileged access rights shall be reviewed regularly in order to verify if they are in line with their duties;

v. Procedures should be established and maintained in order to avoid the unauthorized use of generic administration user IDs, according to systems' capabilities; and

vi. For generic administration user IDs, the of secret authentication information shall be maintained when shared (e.g. changing passwords frequently and as soon as possible when a privileged user leaves or changes job, communicating them among privileged users with appropriate mechanisms).

5.9.4.1 Management of secret authentication information of users

MPSAs shall document a formal management process for the allocation of secret authentication information which shall include the following:

i. Users shall be required to sign a statement to keep personal secret authentication information and to keep group secret authentication information solely within the members of the group;

ii. When users are required to maintain their own secret authentication information, they shall be provided initially with secure temporary secret authentication information, which they are forced to change on use;

iii. Procedures shall be established to verify the identity of a user prior to providing new, replacement or temporary secret authentication information;

iv. Temporary secret authentication information should be given to users in a secure manner; the use of external parties or unprotected (clear text) electronic mail messages should be avoided;

v. Temporary secret authentication information should be unique to an individual and shall not be guessable;

vi. Users shall acknowledge receipt of secret authentication information;

vii. Default vendor secret authentication information shall be altered following installation of systems or software; and

viii. MPSAs shall also use passwords for secret authentication information. Other types of secret authentication information are cryptographic keys and other data stored on hardware tokens (e.g. smart cards) that produce authentication codes.

5.9.5 Review of User Access Rights

MPSAs shall review users' access rights at regular intervals.

The review of access rights shall consider the following:

i. Users' access rights should be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment;

ii. User access rights shall be reviewed and re-allocated when moving from one role to another within the same organisation;

iii. Authorizations for privileged access rights should be reviewed at more frequent intervals;

iv. Privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained; and

v. Changes to privileged accounts should be logged for periodic review.

5.9.6 Removal or Adjustment of Access Rights

a. The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

5.9.7 User Responsibilities

5.9.7.1 Use of Secret Authentication Information

All users shall be advised to:

i. Keep secret authentication information confidential, ensuring that it is not divulged to any other parties, including people of authority;

ii. Avoid keeping a record of secret authentication information, unless this can be stored securely, and the method of storing has been approved;

iii. Change secret authentication information whenever there is any indication of its possible compromise;and

iv. When passwords are used as secret authentication information, select quality passwords with sufficient minimum length and complexity.

5.9.8 System and Application Access Control

5.9.8.1 Information Access Restriction

a. MPSAs shall implement restrictions to access based on individual business application requirements and in accordance with the access control guidelines.

b. MPSAs shall consider the following in order to support access restriction requirements:

i. Providing menus to control access to application system functions;

ii. Controlling which data can be accessed by a user;

iii. Controlling the access rights of users, e.g. read, write, delete and execute;

iv. Controlling the access rights of other applications:

- Limiting the information contained in outputs; and

- Providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.

5.9.8.2 Secure Log-on Procedures

a. MPSAs shall design a procedure for logging into a system to minimize the opportunity for unauthorized access. The log-on procedure shall disclose the minimum of information about the system or application, in order to avoid providing an unauthorized user with any unnecessary assistance.

b. A good log-on procedure shall:

i. Not display system or application until the log-on process has been successfully completed;

ii. Display a general notice warning that the computer should only be accessed by authorised users;

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

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

v. Protect against brute force log-on attempts;

vi. Log unsuccessful and successful attempts; and

vii. Raise a security event if a potential attempted or successful breach of logon controls is detected.

5.9.8.3 Password Management System

a. MPSAs shall establish a password management system

b. The password management system shall:

i. Enforce the use of individual user IDs and passwords to maintain accountability;

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

iii. Enforce a choice of quality passwords;

iv. Force users to change their passwords at the log-on;

v. Enforce regular password changes and as needed;

vi. Maintain a record of previously used passwords and prevent re-use;

vii. Not display passwords on the screen when being entered;

viii. Store password separately from application system data; and

ix. Store and transmit passwords in protected form.

5.9.9 Use of privileged utility programs

a. In case an MPSA is using a utility program, the following guidelines shall be considered and documented:

i. Use of authentication and authorization procedures for utility programs;

ii. Segregation of utility programs from applications software;

iii. Limitation of the use of utility programs to the minimum practical number of trusted, authorised users;

iv. Authorization for ad hoc use of utility programs;

v. Limitation of the availability of utility programs, e.g. for the duration of an authorised change;

vi. Logging of all use of utility programs and documenting of authorization levels for utility programs;

vii. Removal or disabling of all unnecessary utility programs; and

viii. Not making utility programs available to users who have access applications on systems where segregation of duties is required.

5.9.9.1 Access Control to Program Source Code

a. MPSAs shall document the following guidelines to control access to such program source libraries in order to reduce the potential for corruption of computer programs:

i. Where possible, program source libraries shall not be held in operational systems;

ii. The program source code and the program source libraries shall be managed according to established procedures;

iii. Support personnel should not have unrestricted access to program source libraries;

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

v. Program listings shall be held in a secure environment;

vi. An audit log should be maintained of all accesses to program source library.

vii. Maintenance and copying of program source libraries shall be subject to strict change control procedures.

viii. If the program source code is intended to be published, additional controls to help getting assurance on its integrity (e.g. digital signature) should be considered.

5.10 Information Systems Acquisition, In-House Development and Maintenance

5.10.1 Security Requirements of Information Systems

5.10.1.1 Information Security Requirements Analysis and Specification

a. When implementing information system projects, Information Systems related requirements shall be included;

b. Information security requirements shall include:

i. The level of confidence required towards the claimed identity of users, in order to derive user authentication requirements;

ii. Access provisioning and authorization processes, for business users as well as for privileged or technical users;

iii. Informing users and operators of their duties and responsibilities;

iv. The required protection needs of the assets involved, in particular regarding availability, confidentiality and integrity;

v. Requirements derived from business processes, such as transaction logging, monitoring and non-repudiation requirements;

vi. Requirements mandated by other security controls, e.g. interfaces to logging and monitoring or data leakage detection systems; and

vii. Criteria for accepting products shall be defined e.g. in terms of their functionality, which will give assurance that the identified security Requirements are met. Products shall be evaluated against these criteria before acquisition. Additional functionality shall be reviewed to ensure it does not introduce unacceptable additional risks

c. If products are acquired, a formal testing and acquisition process shall be followed.

d. Contracts with the supplier shall address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement, the risk introduced, and associated controls shall be reconsidered prior to purchasing the product.

5.10. 2 Securing Application Services on Public Networks

a. MPSAs shall develop and implement guidelines to secure application services on public networks.

b. The guidelines shall include:

i. The level of confidence each party requires in each other’s claimed identity, e.g. through authentication;

ii. Authorization processes associated with who may approve contents of, issue or sign key transactional documents;

iii. Ensuring that communicating partners are fully informed of their authorizations for provision or use of the service;

iv. 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;

v. The level of trust required in the integrity of key documents;

vi. The protection requirements of any confidential information;

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

viii. The degree of verification appropriate to verify payment information supplied by a customer;

ix. Selecting the most appropriate settlement form of payment to guard against fraud;

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

xi. Avoidance of loss or duplication of transaction information;

xii. Liability associated with any fraudulent transactions; and

xiii. Insurance.

c. Application service arrangements between partners shall be supported by a documented agreement which commits both parties to the agreed terms of services, including details of authorization.

.

d. Resilience requirements against attacks shall be considered, which can include requirements for protecting the involved application servers or ensuring the availability of network interconnections required to deliver the service.

5.10.3 Protecting Application Services Transactions

MPSAs shall develop guidelines for application service transactions that shall 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's secret authentication information of all parties are valid and verified;
   ii. The transaction remains confidential;
   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 are secured;

e. Ensuring that the storage of the transaction details is located outside of any publicly accessible environment, e.g. on a storage platform existing on the organisational intranet, and not retained and exposed on a storage medium directly accessible from the Internet;

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

5.10.4 Security in Development and Support Processes

5.10.4.1 Secure Development Guideline

a. MPSAs shall develop guidelines for secure software development

b. If development is outsourced, the organisation should obtain assurance that the external party complies with these rules for secure development.

c. The guideline shall contain the following:

   i. Security of the development environment;

   ii. Guidance on the security in the software development lifecycle:

   iii. Security in the software development methodology;

   iv. Secure coding guidelines for each programming language used;

   v. Security requirements in the design phase;

   vi. Security checkpoints within the project milestones;

vii. Secure repositories;

viii. Security in the version control;

ix. Required application security knowledge; and

x. Developers’ capability of avoiding vulnerabilities.

5.10.5 Security in Development and Support Processes

5.10.5.1 Secure Development Guideline

5.10.5.1.1 System Change Control Procedures

a. Formal change control procedures shall be documented by MPSAs and enforced to ensure the integrity of system, applications and products, from the early design stages through all subsequent maintenance efforts.

b. The change control procedures shall include but not be limited to:

i. Maintain a record of agreed authorization levels;

ii. Ensure changes are submitted by authorised users;

iii. Review controls and integrity procedures to ensure that they are not compromised by the changes;

iv. Identify all software, information, database entities and hardware that require amendment;

v. Identify and check security critical code to minimize the likelihood of known security vulnerabilities;

vi. Obtain formal approval for detailed proposals before work commences;

vii. Ensure authorised users accept changes prior to implementation;

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

ix. Maintain a version control for all software updates;

x. Maintain an audit trail of all change requests;

xi. Ensure that operating documentation and user procedures are changed

as necessary to remain appropriate;

xii. Ensure that the implementation of changes takes place at the right time

and does not disturb the business processes involved.

5.10.5.1.2 Technical Review of Applications After Operating Platform Changes

a. MPSAs shall document and implement procedures to ensure that when operating platforms are changed, business critical applications are reviewed and tested to ensure there is no adverse impact on organisational operations or security.

b. This process shall cover:

i. Review of application control and integrity procedures to ensure that they have not been compromised by the operating platform changes;

ii. Ensuring that of operating platform changes is provided in time to allow appropriate tests and reviews to take place before implementation; and

iii. Ensuring that appropriate changes are made to the business continuity plans.

5.10.5.1.3 Controls on Software Packages

a. MPSAs shall document guidelines for discouraging changes to software package and limiting to necessary changes in a controlled manner.

b. Where a software package needs to be installed the following points shall be considered:

i. The risk of built-in controls and integrity processes being compromised;

ii. Whether the consent of the vendor should be obtained;

iii. The possibility of obtaining the required changes from the vendor as standard program updates;

iv. The impact if the organisation becomes responsible for the future maintenance of the software as a result of changes; and

v. Compatibility with other software in use.

5.10.5.1.4 Secure System Engineering Principles

a. MPSAS shall establish, document, maintain and review principles for engineering secure information systems implementation efforts;

b. Security shall be designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility.

5.10.5.1.5 Secure Development Environment

a. MPSAs shall develop and implement guidelines for secure development environment which shall address the following:

i. Sensitivity of data to be processed, stored and transmitted by the system;

ii. Applicable external and internal requirements, e.g. from regulations or guidelines;

iii. Security controls already implemented by the organisation that support system development;

iv. Trustworthiness of personnel working in the environment;

v. The degree of outsourcing associated with system development;

vi. The need for segregation between different development environments;

vii. Control of access to the development environment;

viii. Monitoring of change to the environment and program code stored therein;

ix. Backups are stored at secure offsite locations; and

x. Control over movement of data.

5.10.5.1.6 Outsourced Development

.

a. MPSAs shall develop and implement guidelines for outsourced development. The guidelines shall address:

i. Licensing arrangements, code ownership and intellectual property rights related to the outsourced content;

ii. Contractual requirements for secure design, coding and testing practices;

iii. Provision of the approved threat model to the external developer;

iv. Acceptance testing for the quality and accuracy of the deliverables;

v. Provision of evidence that security thresholds were used to establish minimum acceptable levels of security and privacy quality;

vi. Provision of evidence that sufficient testing has been applied to guard against the absence of both intentional and unintentional malicious content upon delivery;

vii. Provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities;

viii. Escrow arrangements, e.g. if source code is no longer available;

ix. Contractual right to audit development processes and controls;

x. Effective documentation of the build environment used to create deliverables;

xi. The organisation remains responsible for compliance with applicable laws and control efficiency verification.

5.10.5.1.7 System Security Testing

a. MPSAs shall document requirements to ensure new and updated systems require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions. For in-house developments, such tests shall initially be performed by the development team. Independent acceptance testing shall then be undertaken (both for in- house and for outsourced developments) to ensure that the system is designed as expected. The extent of testing shall be in proportion to the importance and nature of the system.

5.10.5.1.8 System Acceptance Testing

a. Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

b. System acceptance testing shall include testing of information security requirements and adherence to secure system development practices. The testing should also be conducted on received components and integrated systems. organisations can leverage automated tools, such as code analysis tools or vulnerability scanners, and should verify the remediation of security related defects.

c. Testing shall be performed in a realistic test environment to ensure that the system will not introduce vulnerabilities to the organisation's environment and that the tests are reliable.

5.10.6 Test Data

5.10.6.1 Protection of Test Data

a. MPSAs guidelines shall prohibit the use of operational data containing personally identifiable information or any other confidential information for testing purposes.

b. If personally identifiable information or otherwise confidential information is used for testing purposes, all sensitive details and content shall be protected by removal or modification.

c. The following guidelines shall guide the protection of operational data, when used for testing purposes:

i. The access control procedures, which apply to operational application systems, shall also apply to test application systems;

ii. There should be separate authorization each time operational information is copied to a test environment;

iii. Operational information should be erased from a test environment immediately after the testing is complete;

iv. The copying and use of operational information shall be logged to provide an audit trail.

5.11 Information Security Incident Management

5.11.1 Management of Information Security Incidents and Improvements

5.11.1.1 Responsibilities and Procedures

a. MPSAs shall establish management responsibilities and procedures to ensure a quick, effective and orderly response to information security incidents.

b. Management responsibilities shall be established to ensure that the following procedures are developed and communicated adequately within the organisation:

i. Procedures for incident response planning and preparation;

ii. Procedures for monitoring, detecting, analyzing and reporting of information security events and incidents;

iii. Procedures for logging incident management activities;

iv. Procedures for handling of forensic evidence;

v. Procedures for assessment of and decision on information security events and assessment of information security weaknesses;

vi. Procedures for response including those for escalation, controlled recovery from an incident and communication to internal and external people or organisations;

c. The Procedures established shall ensure that:

1. Competent personnel handle the issues related to information security incidents within the organisation;

2. A point of contact for security incidents' detection and reporting is implemented;

3. Appropriate contacts with authorities, external interest groups or forums that handle the issues related to information security incidents are maintained;

d. Reporting procedures shall include:

i. Preparing 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;

ii. The procedure to be undertaken in case of an information security event, e.g. noting all details immediately, such as type of non-compliance or breach, occurring malfunction, messages on the screen and immediately reporting to the point of contact;

iii Reference to an established formal disciplinary process for dealing with employees who commit security breaches; and

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

5.11.1.2 Reporting Information Security Events

a. All employees and contractors shall be made aware of their responsibility to report information security events as quickly as possible.

b. They shall also be aware of the procedure for reporting information security events and the point of contact to which the events should be reported.

c. Situations to be considered for information security event reporting include:

i. Ineffective security control;

ii. Breach of information integrity, confidentiality;

iii. Information unavailability;

iv. Human errors;

v. Non-compliances with guidelines;

vi. Breaches of physical security arrangements;

vii. Uncontrolled system changes; and

viii. Malfunctions of software or hardware; access violations.

5.11.1.3 Reporting Information Security Vulnerabilities

All employees and contractors shall note and report any observed or suspected information security vulnerability in the systems or services to the point of contact as quickly as possible. This is in order to prevent information security incidents.

5.11.1.4 Assessment and Decision on Information Security Events

a. Information security events shall be assessed and shall be decided if they can be classified as information security incidents.

b. The point of contact shall assess each information security event using the agreed information security event and incident classification scale and decide whether the event shall be classified as an information security incident.

c. Classification and prioritisation of incidents can help to identify the impact and extent of an incident.

d. In cases where the organisation has an information security incident response team (ISIRT), the assessment and decision can be forwarded to the ISIRT for confirmation or reassessment.

e. Results of the assessment and decision shall be recorded in detail for the purpose of future reference and verification.

5.11.1.5 Response to Information Security Incidents

a. MPSAs shall document procedures for response to information security incidents.

b. The response shall include the following:

i. Collecting evidence as soon as possible after the occurrence;

ii. Conducting information security forensics analysis, as required;

iii. Escalation, as required;

iv. Ensuring that all involved response activities are properly logged for later

analysis;

v. Communicating the existence of the information security incident or any

relevant details thereof to other internal and external people or organisations

with a need-to-know;

vi. Dealing with information security vulnerabilities found to cause or contribute

to the incident; and

vii. Once the incident has been successfully dealt with, it should be formally

closed and recorded

c. Post-incident analysis should take place, as necessary, to identify the source of the incident.

5.11.1.6 Learning from Information Security Incidents

a. Knowledge gained from analyzing and resolving information security incidents shall be documented and used to reduce the likelihood or impact of future incidents.

b. There shall 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 should be used to identify recurring or high impact incidents.

5.11.1.7 Collection of Evidence

a. The organisation shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

b. Where available, certification or other relevant means of qualification of personnel and tools shall be sought, to strengthen the value of the preserved evidence.

c. The procedures shall take account of:

i. Chain of custody;

ii. Safety of evidence;

iii. Safety of personnel;

iv. Roles and responsibilities of personnel involved;

v. Competency of personnel;

vi. Documentation; and

vii. Briefing.

5.12 Supplier Relationships

5.12.1 Information security in supplier relationships

5.12.1.1 Information security guideline for supplier relationships

a. MPSAs shall agree with suppliers and document guidelines for supplier's access to the organisation's ICT systems.

b. These controls shall address processes and procedures to be implemented by the MPSAs, as well as those processes and procedures that the MPSAs shall require the supplier to implement, including:

i. Identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the MPSAS will allow to access its information;

ii. A standardised process and lifecycle for managing supplier relationships;

iii. Defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;

iv. Minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organisation's business needs and requirements and its risk profile;

v. Processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation;

vi. Accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party;

vii. Types of obligations applicable to suppliers to protect the organisation's information;

viii. Handling incidents and contingencies associated with supplier access including responsibilities of both the organisation and suppliers;

ix. Resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party;

x. Awareness training for the organisation's personnel involved in acquisitions regarding applicable guidelines, processes and procedures;

xi. Awareness training for the organisation's personnel interacting with supplier personnel regarding appropriate rules of engagement and behavior based on the type of supplier and the level of supplier access to the organisation's systems and information;

xii. Conditions under which information security requirements and controls will be documented in an agreement signed by both parties; and

xiii. Managing the necessary transitions of information, information processing facilities and anything else that needs to be moved and ensuring that information security is maintained throughout the transition period.

5.12.1.2 Addressing Security within Supplier Agreements

a. Supplier agreements shall be established and documented to ensure that there is no misunderstanding between the MPSAs and the supplier regarding both parties' obligations to fulfil relevant information security requirements.

b. The following terms shall be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

    i. Description of the information to be provided or accessed and methods of providing or accessing the information;

    ii. Classification of information according to the MPSAs classification scheme;

    iii. If necessary, also mapping between the MPSAs own classification scheme and the classification scheme of the supplier;

    iv. Legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;

v. Obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;

vi. Rules of acceptable use of information, including unacceptable use if necessary;

vii. Either explicit list of supplier personnel authorised to access or receive the MPSAs information or procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the MPSAs information by supplier personnel;

viii. Information security guidelines relevant to the specific contract;

ix. Incident management requirements and procedures (especially notification and collaboration during incident remediation);

x. Training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures;

xi. Relevant regulations for sub-contracting, including the controls that need to be implemented;

xii. Relevant agreement partners, including a contact person for information security issues;

xiii. Screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;

xiv. Right to audit the supplier processes and controls related to the agreement;

xv. Defect resolution and conflict resolution processes Supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report; and

xvi. Supplier's obligations to comply with the MPSAs security requirements.

5.12.1 Information and Communication Technology Supply Chain

a. Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

b. The following topics shall be considered for inclusion in supplier agreements concerning supply chain security:

i. Defining information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships;

ii. For information and communication technology services, requiring that suppliers propagate the MPSAs security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the MPSAs;

iii. For information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased from other suppliers;

iv. Implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;

v. Implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the MPSAs especially if the top tier supplier outsources aspects of product or service components to other suppliers;

vi. Obtaining assurance that critical components and their origin can be traced throughout the supply chain;

vii. Obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;

viii. Defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the MPSAs and suppliers;

ix. Implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks; and

x. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

5.12.2 Supplier Service Delivery Management

5.12.2.1 MPSAs shall regularly monitor, review and audit supplier service delivery:

This shall involve:

i. Monitoring service performance levels to verify adherence to the agreements;

ii. Reviewing service reports produced by the supplier and arrange regular progress meetings as required by the agreements;

iii. Conducting audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;

iv. Providing information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;

v. Reviewing supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

vi. Resolving and managing any identified problems;

vii. Review information security aspects of the supplier's relationships with its own suppliers;

viii. Ensuring that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

5.13 Business Continuity Management

5.13.1 Information Security Continuity

5.13.1.1 Planning Information Security Continuity

a. MPSAs shall determine whether the continuity of information security is captured within the business continuity management process or within the disaster recovery management process.

b. Information security requirements shall be determined when planning for business continuity and disaster recovery.

c. In the absence of formal business continuity and disaster recovery planning, information security management shall assume that information security requirements remain the same in adverse situations, compared to normal operational conditions.

d. Alternatively, MPSAS could perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations.

5.13.1.2 Implementing Information Security Continuity

a. The MPSAs shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation;

b. MPSAS shall ensure that:

    i. An adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;

    ii. Incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated;

    iii. Documented plans, response and recovery procedures are developed and approved, detailing how the MPSAs will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives.

c. According to the information security continuity requirements, the MPSAs shall establish, document, implement and maintain:

i. Information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;

ii. Processes, procedures and implementation changes to maintain existing information security controls during an adverse situation;

iii. Compensating controls for information security controls that cannot be maintained during an adverse situation.

d. The MPSAs shall co-ordinate with the e-Government Division in implementing their information security business continuity.

5.13.1.3 Verify, Review and Evaluate Information Security Continuity

a. MPSAs shall verify their information security management continuity by:

i. Exercising and testing the functionality of information security continuity processes, procedures and controls to ensure that they are consistent with the information security continuity objectives;

ii. Exercising and testing the knowledge and routine to operate information security continuity processes, procedures and controls to ensure that their performance is consistent with the information security continuity objectives; and

iii. Reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.

5.13.2 Redundancies

5.13.2.1 Availability of Information Processing Facilities

a. MPSAs shall identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures shall be considered.

b. Where applicable, redundant information systems shall be tested to ensure the fail over from one component to another component works as intended.

5.14 Compliance

5.14.1 Compliance with Legal and Contractual Requirements

5.14.1.1 Applicable Legislation and Contractual Requirements

a. All relevant legislative statutory, regulatory, contractual requirements and the MPSA's approach to meet these requirements shall be explicitly documented and kept up to date for each information system and the MPSA.

b. The controls and individual responsibilities to meet these requirements shall also be documented.

c. Management shall identify all legislation applicable to their MPSAs in order to meet the requirements for their type of business.

5.14.1.2 Intellectual Property Rights

The following guidelines shall be considered to protect any material that may be considered intellectual property:

i. Publishing an intellectual property rights compliance guideline with the legal use of software and information products;

ii. Acquiring software only through known and reputable sources, to ensure that copyright is not violated;

iii. Maintaining awareness of guidelines to protect intellectual property rights and giving notice of the intent to take disciplinary action against personnel breaching them;

iv. Maintaining appropriate asset registers and identifying all assets with requirements to protect intellectual property rights;

v. Maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.;

vi. Implementing controls to ensure that any maximum number of users permitted within the license is not exceeded;

vii. Carrying out reviews that only authorised software and licensed products are installed;

x. Providing a guideline for maintaining appropriate license conditions;

xi. Providing a guideline for disposing of or transferring software to others;

xii. Complying with terms and conditions for software and information obtained from public networks;

xiii. Not duplicating, converting to another format or extracting from commercial recordings (audio) other than permitted by copyright law; and

xiv. Not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.

5.14.1.3 Protection of records

To meet these record safeguarding objectives, the following steps should be taken within an MPSA:

i. Guidelines shall be issued on the retention, storage, handling and disposal of records and information;

ii. A retention schedule shall be drawn up identifying records and the period for which

they shall be retained in accordance with policy, legal and regulatory provisions;

iii. An inventory of sources of key information shall be maintained.

5.14.1.4 Privacy and Protection of Personal Information

An MPSAs' data guideline for privacy and protection of personal information shall be developed and implemented in line with the existing laws on Data Protection and Personal privacy. This guideline shall be communicated to all persons involved in the processing of personal information.

5.14.1. 5 Regulation of Cryptographic Controls

Legal advice shall be sought by MPSA to ensure compliance with relevant legislation and regulations when using cryptography.

5.14.1.6 Information Security Reviews

a. Management shall initiate the independent review. Such a review shall be carried out by individuals independent of the area under review.

b. The results of the independent review shall be recorded and reported to management. These records shall be maintained.

c. If the independent review reveals that the MPSAs approach and implementation to managing information security is inadequate, e.g. documented objectives and requirements are not met or not compliant with the direction for information security stated in the information security guidelines, management shall consider corrective actions.

5.14.1.7 Compliance with Security Guidelines and Standards

a. Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security guidelines, standards and any other security requirements.

b. Managers shall identify how to review that information security requirements in guidelines, standards and other applicable regulations are met. Automatic measurement and reporting tools shall be considered for regular review.

c. If any non-compliance is found as a result of the review, managers shall:

   i. Identify the causes of the non-compliance;

   ii. Evaluate the need for actions to achieve compliance;

   iii. Implement appropriate corrective action; and

   iv. Review the corrective action taken to verify its effectiveness and identify any weaknesses.

5.14.1.8 Technical Compliance Review

a. Technical compliance shall be reviewed preferably with the assistance of automated tools, which generate technical reports for subsequent interpretation by a technical specialist. Alternatively, manual reviews (supported by appropriate software tools, if necessary) by an experienced system engineer could be performed.

b. If penetration tests or vulnerability assessments are used, caution shall be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeated.

c. Any technical compliance review shall only be carried out by competent, authorised persons or under the supervision of such persons.

5.15 Application Access Control

a. MPSAs shall adhere to strict application access control guidelines which clearly define the following:

i. Access application system functions shall be restricted in accordance with the access control Guidelines of the MPSA.

ii. Access to the application should be based on a need to know basis and formal access from the application owner.

iii. Restrictions to access shall be based on individual business application requirements.

c. The following shall be considered in order to support access restriction requirements:

i. Provide menus to control access to application system functions;

ii. Control which data can be accessed by a particular user;

iii. Control the access rights of users, e.g. read, write, delete and execute; iv.

Control the access rights of other applications;

v. Limit the information contained in outputs; and

vi. Provide physical or logical access controls for the isolation of sensitive applications, application data, or systems.

5.15.1 Access Card, ID Cards

Access to the Institutions' premises needs to be controlled through appropriate access control and authentication mechanisms. All members of staff need to be issued a staff identification card/access cards that shall always be worn visibly.

5.15.2 Locks and Safes

All media containing confidential information needs to be kept in safes where access is strictly controlled.

5.15.3 Surveillance & Alarm System

The premises of the MPSAs need to be equipped with the appropriate surveillance alarm systems that are operational on a 24x7 basis.

5.15.4 Network Access Controls

a. Identify networks and network services which are allowed to be accessed;

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

c. Identify management controls and procedures to protect access to network connections and network services which include:

   i. The means used to access networks and network services (e.g. Use of virtual private network or wireless network);

   ii. User authentication requirements for accessing various network services; and

   iii. Monitoring of the use of network services.

5.15.5 Remote Access (VPN)

a. Identify the communications security requirements, taking into account the need for remote access to the internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system.

b. Provide 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 stakeholders are authorised to access.

5.15.6 Biometrics

Make use of biometric mechanisms in line with legal requirements and relevant Public Sector guidelines pertaining to the security around personal information.

5.15.7 Web Application Firewalls (WAFs)

a. Adhere to the following standards when implementing web application firewalls:

   i. Most WAFs have a set of pre-built Guidelines to ensure that devices are secured against the most commonly identified application security risks.

ii. Public Institutions shall configure these appliances in a ‘learning mode’ whereby the devices learn the application calls that are authorised during setup and testing phases.

iii. The WAF shall be configured to analyze inbound and outbound data and decide to block or permit specific elements.

b. Database Security Conduct a review of the key security controls implemented in the databases. The assessment shall include reviewing database server configuration parameters, operations and related procedures and shall cover the following areas:

i. Access controls and allocation of privileges;

ii. Usage of privilege accounts;

iii. Auditing, logging and monitoring;

iv. DBMS configuration;

v. OS access and user management;

vi. Roles allocation;

vii. Backup and recovery;

viii. Password management;

ix. Database Security patches management;

x. Roles and Grant allocation;

xi. User tracking method and implementation;

xii. Username and password structure; and

xiii. Standards for views and roles.

5.16 Document Review

In order to keep abreast of progress in industry, Information Security Standards shall be regularly reviewed.

Suggestions for improvements to published standards, addressed to the National Coordinator, e-Government Division are welcome.

6.0 ATTACHMENTS

Appendices to be attached to MPSAs Information Security Guidelines include;

i. Internal Contacts – Information Security Team;

ii. Information System Suppliers and Contacts; and

iii. Out of Hours Support Arrangement