dhsps&l
Department:
Human Settlements, Public Safety & Liaison
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF PUBLIC SAFETY

ICT ENTERPRISE POLICY DOCUMENT

Document ID:	**ICT2010/001**	
Version:	**1.0**	
Effective Date:	***December 2012***	
Document Status:	First Draft for Directorate Review	
Revision frequency:	Annually	
Applicability:	Dept Of Public Safety	
Directorate:	Strategic Support Services (ICT)	
Owner:	Dept Of Public Safety	
Document Approval:	**Signature**	**Date**
Director: Strategic Support Services		
Head Of Department: Dept Of Public Safety	26/11/2012	26/11/2012

Revision Record

Revision Number:	Description	Change Request status:	Revision Date:
0.1	Draft ICT Enterprise Policy	Draft	
1.0	Draft for the Directorate review	Review	

Electronic Record

Folder Name:	Folder and File Path
ICT-QA	C:/Documents and settings/Department/ Policies*(currently)*

Electronic Component File

File Name:	Description	Generated Source
ICT2010-001	Draft ICT Policy Document	MS Word 2007

Author/Editor

Author/Editor:	Name:	Functional Area
Author	**Ms G Mogale**	**Assistant Director: Information Systems**
Editor	**Mr. S Cloete**	**Deputy Director: ICT Manager**
Editor	**Mr. S Matlhako**	**Director: Strategic Support Services**

Reviewers

Ref	Reviewer	Functional Area
1	Mr. S Matlhako	Strategic Support Services
2	Mr. S Cloete	ICT Services Management
3	Ms. G Mogale	Information Systems
4	Mr. T Taiwe	E- NaTIS security
5	Mr. L Mangonyane	Minimum Information Security Standard
6.	Mr. E Jimla	Records Management
7.	Ms. N Mphahlele	Strategic Planning

This draft document will be distributed to all relevant stakeholders.

Table of Content Page

Preamble

The information age demands that government be flexible and respond speedily to citizens' demands for services. This era is characterized by, what we would call information overload and the need to share data and information within and across government departments.

The government long term objectives are to improve productivity, lower costs, and bring about citizens' convenience in delivering services. To achieve this government cannot continue to spend on technology without benefits or improvement to service delivery.

For technology to be a true business enabler, technology must support business. This requires that CIO's/Managers understand their departmental environment and plan systems that are aligned to their departmental mission and objectives. These systems must help must help government achieve its long-term objectives.

In the lieu of the above the North West Department of Public Safety Information Technology Department having it been fully aware of the need and comprehensive environment has envisaged a process of planning and mapping technology to support business objectives which is guided by this policy document.

Systems planning aims to integrate the following to the benefit of the Department of Public Safety:

- Human Resources (People)
- Data and Information
- Business activities and Processes(Infrastructure and networks)

1. Acronyms and Definitions

ICT:	Information and Communication Technology
ITP:	Information Technology Planning
DPS:	Department of Public Safety
IT:	Information Technology
MISS:	Minimum Information Security Standard
MIOS:	Minimum Interoperability Standard
ITIL:	Information Technology Infrastructure Library
PC:	Personal Computer
DAA:	Designated Accrediting Authority
COTS:	Commercial off the Shelf
HOD:	Head of Department
ITS:	Information Technology System
IM:	Information Management
CMOS:	Complementary Metal-oxide Semi-Conduct
GITOC:	Government Information Technology Officer Council

Definition of Terms:

Mechanism testing:	Testing of security mechanism such as identification and verification.
Interface testing:	Testing of all user routines that call up security functions.
Penetration testing:	Testing of security during development cycle.
Detrimental software:	Harmful Software
Special privileges:	Privileges enabling users to override system or application Controls
IP:	Internet Protocol

2. Purpose and Objectives

2.1 The purpose of this document is to guide managers and employees in the Department of Public Safety in the implementation of control measures aimed at integrating employees, Information/Data and Technology together to the benefit of DPS in terms acceleration, effectiveness and efficiency of service delivery. This policy relates to all IT facilities and services provided by DPS. All staff and volunteers are expected to adhere to it.

2.2 The policy objectives include to:

(i) Ensure that IT facilities are used:

Legally, securely, without undermining DPS, effectively, in a spirit of co-operation, trust and consideration for others, so they remain available.

(ii) Enable business objectives using technology.

(iii) Ensure that security is built into IT systems of the DPS.

(iv) Protect the PC configuration of DPS against sabotage, espionage and actions endangering security.

(v) Safeguard DPS data and information contained within systems against unauthorized access.

(vi) To reduce risk of human error and to prevent its personnel and contractors from committing sabotage, espionage subversion or actions posing security risks or from being subjected thereto within IT system environment.

3. Principles

As public service gears itself for the electronic government mode of service delivery, the need for a different breed of information security in the public service becomes imperative.

This is as a result of possibilities of integrated government services that will rely heavily on the information security of each and every component of electronic government services can cause crippling effects on the service delivery by the public service, with major inconveniences to the users of services.

The strategic and critical value of public service information and hence the protection thereof, needs appropriate legal recognition.

The following principles shall govern the use and management of external overt electronic information sources:

3.1 **Compliance with all applicable legislation**, Regulation and policies. Access to computer systems and networks owned or operated by DPS impose certain responsibilities and obligations on users/employees and is subject to applicable legislation such as Copyright Act, 1978 (Act No 98 of 1978).

3.2 **Conformity with Ethos Standard**. Acceptable use shall always be ethical, reflect honesty, and show restraint in the consumption of shared resources. It shall demonstrate respect for intellectual property, ownership of information, system security mechanisms, and the individual's rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance.

3.3 **Subject to monitoring**. Use of network and services provided by an institution may be subject to monitoring for security and/or network management reasons that include ensuring that the expenditure resulting from the utilization of commercial databases reflects the value of the information for the DPS.

3.4 **Preference of Official Use**. The workstations owned and operated by employees of the DPS shall mainly be used for official purposes and such usage shall be given preferential access and computer time. The usage of internet facilities must therefore conform to the purpose, goals and mission of the DPS and the execution of each user's official job description responsibilities.

3.5 **Acceptance of Personal Liability**. Users, who violate any copyright declarations, unless specifically required by official duties, are acting outside the course and scope of their employment or other authority and the DPS is relieved of any legal responsibility for such actions. Users will be personally responsible and liable for infringing activities. Therefore, by participating in the use of networks and systems provided by the department, users agree to be subject to and abide by this policy for their use. Users agree to assume the responsibility for any charges associated with billable services unless appropriate authorization has been obtained. Willful violation of the principles and provisions of this policy may also result in disciplinary action.

3.6 **DPS envisage that all personnel with internet access including e-mails are aware** of, and will comply with, an acceptable code of conduct in their usage of the internet in addition to compliance with each DPS information security policies.

3.7 **DPS shall manage IT effectively and efficiently**, with Batho Pele principle informing the acquisition, management and use of IT. DPS uses IT to leverage service delivery, and IT shall not acquire for its sake.

4. Legislative Framework

4.1 This policy is underpinned by SA Laws, international norms and standards, and best practices.

4.2 The framework includes the following:

4.2.1 Constitution of the RSA;

4.2.2 Public Service Act, 1994 and Regulations;

4.2.3 Information Security Act, Government Gazette vol. 449;

4.2.4 Promotion of access to information Act;

4.2.5 SITA Act 88 of 1998

4.2.6 Green Paper on Electronic Commerce for South Africa;

4.2.7 MISS

4.2.8 MIOS

4.2.9 COBIT

4.2.10 ITIL

4. Legislative Framework

4.1 This policy is underpinned by SA Laws, international norms and standards, and best practices.

4.2 The framework includes the following:

Acts	Brief Description
1. Constitution of the RSA, No. 108 of 1996	**Access to information:** • Everyone has access the right of access to information held by the state, and information that is held by another person and that is required for the exercise or protection of any rights. • National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.
2. Information Security Act, Government Gazette Vol. 449	• To promote convergence in the broadcasting, broadcasting signal distribution and telecommunications sectors and; • To provide the legal framework for convergence of these sectors; • To make new provision for the regulation of electronic communications services, electronic communications network services and broadcasting services; • To provide for the granting of new licenses and new social obligations; • To provide for the control of the radio frequency spectrum; • To provide for the continued existence of the Universal Service Agency and the Universal service

	Fund; • And to provide for matters incidental thereto.
3. Promotion of access to information Act 2 of 2000	• To give effect to the constitutional right of access to any information held by the State and any information that is held by another person and requires for the exercise or protection of any rights; • And to provide for matters connected therewith.
4. SITA Act 88 of 1998	• To provide for the establishment of a company that will provide information technology, information technology systems and related services to, or on behalf of, participating departments and in regard to these services, act as an agent of the South African Government; • And to provide for matters connected therewith.
5. Green Paper on Electronic commerce for south Africa, November 2002	• Provides for Provincial Governments the platform from which to translate topical issues around e-commerce into government policy. • It is a consultative document designed to raise questions on issues that need to be addressed by Government policy formulation process. The document is aimed at the following benefits (Amongst others) to the Provincial Government: • Improved response time: Quick and cost efficient way through which to communicate. • Improved customer service: Information is shared more quickly through the user of an electronic medium. • Ease of concluding deals and financial transactions: Click-and-

	Pay technology is gaining popularity as a means through which to transact. Published information, communicating, buying, selling, paying and checking orders occurs 24 hours a day, 365 days a year.
6. Minimum Information Technology System Security Standards (MITSSS)	• The document describes the minimum security requirements to be adhered to in the process of acquiring information technology systems to ensure that security is built into the IT systems of Government.
7. Control Objectives For Information Technology (COBIT *(Best Practice)*)	• This is framework that provides good practices for the management of IT processes in a manageable and logical structure, meeting the multiple needs of business management requirements. • The framework enables the development of clear policy and good practices for IT control through the department.
8. Minimum Interoperability Standards for Information System(MIOS)	• This are standards intended to set out the government's technical principles and standards for achieving interoperability and information systems coherence across the public sectors. • It defines the essential prerequisite for joined-up and web enabled Government. • Next to security it is an essential component in the overall e-Government strategy. • The adherence to the MIOS standards and policies is mandatory as set out in the proposed chapter five of the Public Service Regulations.

9. Information Technology Infrastructure Library (ITIL) Version 3 *(Best Practice)*	• This is the approach to IT service management in the world. • It provides a cohesive set of best practice, drawn from the public sectors internationally

5. Sphere of Application

This policy is applicable to all employees of DPS in terms of Public Service Regulation of 2002, Service Providers (Consultants and Contractors) and Partners.

6. Policy Statement

This policy seeks to address the following areas:

- Systems acquisition, development and testing
- System operation
- Internet connection
- Intranet connection
- Intranet website security
- Modem / dial-up computer connection
- Disposal of computer-related articles
- ICT physical security
- Personnel security

6.1 System acquisition, development and testing

6.1.1 System Requirements Specification

The user requirements for new systems or enhancements to existing systems shall specify security objectives of the system as well as the security control requirements, including the need for contingency requirements.

6.1.2 Design Specification

The preventative, detection, corrective security control requirement specification that protect hardware, programs, and data against deliberate or negligent changes, destruction, sabotage or espionage shall be integrated into the system acquisition plan incorporated into the design specification of the system.

The design shall consider the following security control:

(a) Security Architecture.

(b) Security Grading.

(c) Identification and Authentication.

(d) Non-reputation.

(e) Confidentiality.

(f) Control.

(g) Integrity.

(h) Recovery/Availability.

(i) Audit-ability/Accountability.

(j) Separation of Functionality.

(k) Source Data.

6.1.3 Security Testing Plan

- A security testing plan shall be drawn up for the testing of all the security features to ensure that the system operates as described in the document. The detail regarding what must be tested and what equipment will be used shall be documented. All security aspects in respect of the system shall be documented in full and the documentation shall be updated regularly for submission to the Designated Accrediting Authority (DAA).
- Development and testing activities shall be separated as far as possible. The system developer shall test all the security features and ensure that the system operates as documented. **Mechanism testing** as well as **interface testing** shall be executed.
- The testing of security measures shall be continued during the SLC to ensure that the security objectives are met and that controls operate as intended. Where necessary, enhancements or modification shall be made and documented.
- Live sensitive data or files shall not be used to test applications software until the software integrity has been reasonably assured by testing with non-sensitive data or files.
- Sensitive application software will not be placed in a production status until the system tests have been successfully completed and the application has been properly certified and accredited.

6.1.4 System Development, Changes and Implementation

Supervisory personnel must ensure that proper segregation of duties applies to all areas dealing with systems development, systems operations, or systems administration.

6.1.4.1 **Development Specifications**

I. Development, Test and operational facilities shall be separated to achieve segregation of roles involved and to prevent accidental changes or unauthorized access to operational software and data. Development and operational software shall, where possible, run on different computer processors or in different domains or directories.

II. Control measures and procedures for the protection of programs and data shall be built in, tested and audited environment to ensure that data and programs cannot be changed without authorizations, destroyed or subjected to sabotage and/ or espionage due to negligence or on purpose.

III. All systems / programs shall meet the prescribed security requirements and programming standards. Master software and documentation shall be stored separately. The development of systems shall not be done with live data unless it is transferred to a separate test system. Databases containing personal data shall be depersonalized before use. No unauthorized temporary amendments (patches) shall be made to production and /or operational programs.

IV. Before acceptance and accreditation of a system by the DAA in accordance with the requirement standards, an audit of the security measures shall be conducted by an appropriate mechanism established by the DAA for this purpose. It shall be certified that the system configuration meets all the security requirements and programming standards and that the security manual has been updated. All security audit actions shall be documented.

V. All emergency maintenance programs e. g trapdoors, super-zaps, patches etc shall be removed before a system is installed. Systems shall be audited for harmful software e.g logic bomb before installation and implementation.

VI. All new and enhanced systems must be fully supported at all times by comprehensive and up to date documentation. New systems or upgraded systems should not be introduced to the live environment unless supporting documentation is available.

6.1.4.2 **Change Control**

I. The integrity of the organization's operational software code must be safeguarded using a combination of technical access controls and restricted privileges allocation and robust procedures. Formal change control procedures must be used for all amendments to systems, with comprehensive audit trail to control Program Source libraries and versions of old programs. All changes to programs must be properly authorized and tested by qualified personnel in a test environment before moving to the live environment.

II. Patches to resolve software bugs may only be applied where verified as necessary and with management authorization. They must be from a reputable source and are to be thoroughly tested before use.

III. Strict control shall be applied to system /program changes after an overview/code walk through and system testing. Changes shall only be made according to predetermined procedures and by authorized people. An audit trail shall be kept with all the relevant information about the changes to the programs/systems.

IV. Systems shall be re-certified in the following instances:

- When substantial changes have been made to the system;
- When changes in the requirements result in the need to process data of a higher sensitivity;
- After the occurrence of a serious security violation which raises question about the validity of an earlier certification; and
- Without exception no less frequently three years after the previous certification.

V. All systems shall be re-accredited when major changes occur first. Prior to re-accreditation, an evaluation team established by Head of the government institution responsible for IT security shall conduct an IT security verification review.

6.1.4.3 **Security Manual**

I. Security manual shall be compiled at the start of the system development phase. All security aspects in respect of the system shall be documented in the system security manual to ensure that prescribed security measures are adhered to.

II. Limitations in respect of the use of system interfaces shall be defined and incorporated into the security manual. Management and administrative control measures, which ensure the correct application of the system interfaces, shall be documented.

III. The security manual shall be updated after each system/program change.

6.1.4.4 System Implementation

I. The implementation phase starts when the acquisition of the product or service has been finalized and ends when the system has been accredited, implemented and accepted by the requestor.
II. All computer hardware and software shall be implemented in terms of an implementation plan. The implementation plan shall be coordinated by the system owner and shall be compiled in conjunction with the developer.
III. The implementation plan shall also address the activities related to the coordination and implementation of the security measures and specify acceptance criteria to be met before the system is put into operation. Acceptance criteria shall be clearly defined, agreed, documented and tested.

6.1.5 Procurement of Computer-Related equipments and Software

Procurement objectives

- All equipment to be purchased through Supply Chain Management.
- All requests should be written to Strategic Support Services.
- All end user requests accompany the approval of the programme manager or director in question.
- All standards to be adhered to as set out per SITA tenders 285.
- Electronic equipment not specified in SITA Tenders require 3 quotations.
- Supply Chain Management procedures be adhered to as contained in Policy.

Procurement standards

- ICT Requests received by the Information Technology section to be processed monthly.
- Quotations to be sourced by (IT) Strategic Support Services with lead time of 5 (Five) days.
- IT to prepare draft submission for signatories lead time 5 (Five) days.
- Strategic Support Services to prepare requisition (VA2) 1(One) day. Supply Chain Management to approve requisition (VA2) 2 (Two) days.
- Supply Chain Management to generate order 2(Two) day.
- Supplier delivery of equipment 2 (Weeks).
- Following receipt of invoice payment to be concluded
- Under no circumstance should ICT equipment be issued from stores without the consent of IT.
- Newly acquired ICT assets to be delivered by SCM asset management section.
- Order to be generated per ICT request / submission.

Equipment standards

- Desktop computers are provided to employees who are in administrative, financial and office management posts and who are office bound by the very nature of their jobs.

Allocation

- A user will either be allocated a laptop or a desktop computer and not both (This applicable to all levels)

Replacement

Consideration to the following will be given

- Age PC – 3 Years
  Laptop – 2 Years
- Hardware / Firmware fault
- Replacement for specific requirement for hardware or system.
- Fault persists after full format.

Following will prevail

- Written motivation by line manager
- Inspection form be supplied regarding fault
- Approval through Strategic Support Services for replacement.

SOLICITATION PROCESS

Sourcing of quotations

- Strategic Support Services to source quotations as per SITA 285 specifications.
- Quotations sourced from vendors have a turnaround time of five (5) days.
- ICT request sheet with indicated specifications to be used for sourcing quotations.
- Where three (3) Quotations have been requested and only two received after turnaround time expiration then only two submitted be considered.
- Cheapest will quote will prevail providing quality and standards as set out per SITA Tender 285 prior being delivered.

DEPLOYMENT

Computer control standards

NEW ASSETS

- Delivery of ICT procured equipment including electronic external devices that are deemed as consumable's by asset management should be accepted by Supply Chain Management where the asset will be noted in registry and signed for by Information Technology on withdrawal of equipment .

- Delivery note / invoice to be signed by Strategic Support Services and equipment delivered be verified up against order / invoice by asset management.
- Supply Chain Management to barcode equipment 2 (days) after payment has been made.
- IT equipment to be kept in store for initial configuration.
- 3 day period for configuration.
- On completion client to be notified and must be collected and signed for and taken up on asset by SMC then delivered to and or collected by the relevant official as well as signed for.
- In the case of Supply Chain Management ICT deployment IT be notified and must be accompanied by a IT technician for installation purposes.
- Any movement of ICT equipment to be managed, maintained by SCM Asset Management section and reported to Strategic Support Services Information Technology section.

POOL EQUIPMENT

ICT / electronic equipment to be retained and managed by stores

- IT to be notified when issuing or accepting ICT equipment
- IT Asset form to be signed and submitted to IT for record purposes.

6.1.5.1 Commercial off the Shelf (COTS) Products

i. DPS should avoid the selection of business critical software which has not been adequately proven. The selection process for all new business software must incorporate the criteria upon which the selection will be made. Such criteria must receive the approval of senior management and should be complaint with the MIOS standards provided.
ii. All purchases of new systems hardware or new components for existing systems must be made in accordance with appropriate information security standards and other DPS's policies, as well as technical standards. No procurement of computer-related equipment and software shall take place without appropriate approval from the designated official responsible for IT management and support. This includes free software.
iii. Only software as prescribed and/or approved, and that comply with the security standards stipulated in this policy and standards guide shall be used on the DPS computers.

6.1.5.2 Self-developed Software

i. Request for the writing of own programs for the improvement of local procedures shall be submitted to the designated official responsible for IT management and support for approval and authorization and shall contain full particulars of the intended application.
ii. The program, plus source code, shall be subjected to certification in accordance with the appropriate procedures (accreditation) and standards by DAA in order to apply quality control to development process and to facilitate adequate configuration management of the intended application.
iii. The program shall not interfere or be in conflict with the existing laid down systems. Development with live data shall not be implemented before full compliance with the provisions for accreditation thereof has been met.
iv. All programs developed in this way shall remain the property of the DPS that holds the copyright and shall not be marketed in the private sector without authorization. An application for a commercial license for any such product(s) shall, in writing, be directed through appropriate management channels to the HOD of DPS, or his/her delegate.
v. System owners shall keep a system register in respect of all programs developed in their own structure.

6.2 System Operator

6.2.1 Document Operating Procedures

- System operating procedures shall be documented and maintained to ensure the correct and secure operation of information processing facilities. The procedures shall specify the instructions for the detailed execution of each job including processing and handling of information, scheduling requirements, error handling, use of system utilities, output handling and disposal, back-up, equipment maintenance, system restart and recovery.
- Version control procedures should always be applied to documentation belonging to the DPS or its customers.

6.2.2 Assets Classification and Control

- All major information technology system assets shall be classified and accounted for and recorded in an asset register by the IT management and support structure of DPS in accordance with applicable policies of the institution.
- The asset register is to be kept up-to-date and readily available to the staff that is authorized to support or maintain systems.

6.3 Configuration Management and Change Control

6.3.1 Configuration Management

a. In order to prevent sabotage, espionage, subversion and actions endangering security, effective configuration management shall be applied throughout the life cycle of all IT systems.
b. The influence and impact of a change to a configuration item on the system and system interfaces shall be determined and controlled.
c. IT system and network configurations shall be documented. The current state of a system configuration shall be known at any given time.
d. Users shall not modify a system configuration. For this, the following features shall be incorporated either within the hardware or operating system software of DPS's systems:
    I. Users will be allowed to access only the memory locations, files, and peripheral devices that have been allocated to the user by the operating system.
    II. Computers, other than stand-alone PCs, shall have the capability to effectively isolate users from one another and from the operating system.
    III. Any attempt to execute an illegal instruction shall result in a hardware interrupt permitting the operating system to interrupt and abort the program containing the instruction.
    IV. Error detection and memory boundary checking should be performed on transfers of data between memory, peripherals and external devices.
    V. Automatic programmed interrupts must control system malfunctions and operator errors.

e. No computer hardware linked to a communication network shall be moved/removed without the written authorization of the System Manager. If the movement of hardware also entails changes to the communication network, the cancellation and reactivation of system component addresses and user rights shall take place at the same time.
f. Configuration management shall ensure that any additions, omissions and/or changes made to the system correspond with the set security measures.

6.3.2 Change Control

I. The System Manager shall ensure that standards and procedures for controlling proposed changes to the ITS environment are established. Wherever practicable, application and operational change control procedures shall be compiled with to ensure that no unauthorized changes to equipment, programs, software or procedures can be made.

II. Before a system amendment/changes can be made, control measures and procedures shall be in place to ensure that the change has been authorized and that the data is protected against deliberate or negligent changes, destruction, sabotage and/or espionage

III. Amendments to systems, programs and system interfaces in operation shall be controlled according to predefined standards and formal approval procedures. Change detail shall be communicated to all relevant persons.

IV. When changes have been made to system, the amendment shall be tested and the system documentation shall be updated accordingly. A version for all software updated shall be maintained. Amendments shall not contain detrimental software.

V. An audit trail shall be kept with all relevant information about the changes to the system/program.

VI. The security procedures shall identify responsibilities for aborting and recovering unsuccessful changes.

6.3.3 Information Back-Up

- Appropriate procedures shall be established for the making of back-up copies of essential business information and software to ensure that it can be recovered following a disaster or media failure. Back-Up arrangements for individual systems shall be regularly tested to ensure that they meet the requirements of business continuity plans stipulated in this policy.
- Back-up media shall be regularly tested, where practical, to ensure that they can be relied upon for emergency use when necessary. Back-up copies shall be stored off-site and be given an appropriate level of physical and environmental protection consistent with the standards at the main site.
- The retention period for back-up copies of essential business information shall be determined and documented.

6.3.4 Use of System Utility

The system utility program (e.g monitoring /sniffing tools) use that might be capable of overriding system and application controls shall be restricted to authorized officials and tightly controlled. Monitoring/sniffing tools may only used with the approval of the designated official responsible for IT security and the respective line functional structures within DPS. System utility shall be protected by passwords/authentication procedures and segregated from applications software. An audit trail of all system changes made by these utilities shall be kept.

6.3.5 System Maintenance

6.3.5.1 Maintenance Contracts

- All contractors concerned with the maintenance DPS's systems shall have the appropriate security clearances before a contract may be concluded.

6.3.5.2 Hardware / Software Maintenance

- The maintenance of hardware and software shall only be done by authorized contractors. System Managers are responsible for computer equipment used in their respective areas of responsibility. All users shall ensure that computer hardware and software are handled and used in accordance with vendor specifications.

6.3.6 Outsourced Processing

- Persons responsible for commissioning outsourced computer processing must ensure that the services used are from reputable companies that operate in accordance with quality standards which should include a suitable SLA which meets the requirements of the DPS.

6.3.7 Security of System Documentation

6.3.7.1 Access to System Documentation

- Complete, updated system manuals/operating procedures shall be available to authorized operators, programmers, system analysts, users and auditors where applicable. The System Manager shall authorize the access list for users who may gain access to specific system documentation.
- Users and operational personnel shall not be given access to program documentation. Rights shall be allocated per user e.g read, write etc

6.3.7.2 Security Classification

- Applicable security classifications shall be allocated to all system documentation and be controlled, handled distributed, stored and disposed of in accordance with the allocated security classification.

- System documentation held on/supplied via a public network shall be appropriately protected. Back-up copies shall be made of all system documentation and stored safely off-site in accordance with applicable DPS policies on the management of its software assets.

6.3.8 System Access Control

- Access to the computer systems and information of DPS shall be controlled by means of an approved computer access control system that identifies and verifies/ authenticates the identity, and if necessary, the terminal or location of each authorized user. The following measures and procedures shall, where appropriate, be implemented to control the allocation of access rights to the systems and services:
  I. Discretionary Access Control
     When using discretionary access control, the resource owner shall be responsible for the protection of his/her files by specifying who may gain access to them and how, when and under what conditions they may be accessed.
  II. Mandatory Access Control
      I. Access to multi-user information services shall be controlled through a formal user registration process. Unique user IDs shall be allocated so that users can be linked to and made responsible for their actions. The use of group IDs shall only be permitted where they are suitable for the work carried out.
      II. A user shall meet the minimum security requirements of the job before registration as a system user. The level of access granted shall be based on the need-to-know principle and shall not comprise segregation of duties. A security profile shall be determined and compiled for every user, based on what systems) /data field(s) the user requires access to as well as his/her security clearance.
      III. A formal record shall be maintained of all registered users. The appropriate access rights (or privileges) must be recorded in an Access Control List. Such records are to be regarded as classified documents and safeguarded accordingly. Access rights and user IDs of users who have changed jobs or left the DPS shall immediately be removed and not be issued to other users.

III. Secure Logon

Access to ITS services shall be via a secure logon process. The users of the system shall be identified uniquely by means of a user/biometric

identification. After the correct user identification, a password shall be given. The secured logon process shall comply with the following security requirements:

- System or application identifiers shall not be displayed until the logon process has been successfully completed.
- Help messages shall not be provided during the logon procedure that would aid an unauthorized user.
- The logon information shall be validated only on completion of all input data. If any error condition arises, the system shall not indicate which part of the data is incorrect.
- The number of unsuccessful logon attempts shall be limited to the three before action is taken to force a time delay before further logon attempts are allowed; disconnect data link connections; and/or sound an alarm at the Network Manager.

IV. Privilege Management

Access privilege shall be based on a legitimate need to have system access. Every user shall be given only the minimum computer-related privileges that will enable him/her to perform his/her functions effectively. The use of special privileges shall be restricted and controlled through a formal authorization process, allocated on a need-to-use and event-by-event basis and revised at regular intervals. Special privileges shall be assigned to a different user identity from those used for normal business use. A record of all special privileges allocated shall be maintained. Privileges that have not been specifically granted shall be denied.

V. Cancellation of Access

- If a user does not use the system(s) for 30 days, access shall be suspended automatically by the system and the user shall be removed from the system after 6 months. If the user no longer needs partial or complete access to the information on the computer system(s) e.g transfer and change of job description, etc, the access authorization of such a user shall be cancelled or amended immediately. Access to the system shall be suspended after three unauthorized efforts to gain access to the system and/or expiry of the user's security clearance. Terminals in high-risk environments shall shut down after a pre-defined period of inactivity to prevent unauthorized access. Clearance out procedures shall make provision for an employee to be removed from the system(s).
- In the case of resignations/retirements, access to a SECRET and/or TOP SECRET system(s) shall be terminated third days before the last

working day. In the case of dismissals, access to all systems shall be terminated immediately and when possible prior to notifying the affected member of the pending action.

VI. Access Audit Trail

- The access control system shall update an audit trail of all authorized as well as unauthorized efforts to gain access to computer systems and shall be monitored by the System Manager/delegate regularly enough to minimize damage or illegal entries. Critical aspects of system security shall be monitored real-time. Unauthorized access attempts shall be handled as a breach of security. The following security-related activities shall be captured in an audit trail:
  i. All efforts, whether valid or invalid, to gain access to a system.
  ii. All requests, authorized or unauthorized, for access to protected programs, data and transactions.
  iii. All amendments of sensitive and classified data and programs.
  iv. All changes in privileges or security attributes.
  v. All sign-on and sign-off transactions, whether successful or unsuccessful.
  vi. The following relevant data shall be recorded for every activity noted:

    - Date and time of logon and logoff
    - Identification of user who initiated the activity
    - Type of activity
    - Successful or unsuccessful effort.
    - Origin of the request eg PC MAC address
    - Name of the object concerned.
    - RESTRICTED intrusion / interception detection.

- Real-time intrusion detection software/mechanisms shall be implemented in Secret and TOP SECRET systems to help defend the system against attacks that succeed in invading or penetrating its preventative mechanisms. The alerts raised by the intrusion detection mechanism(s) shall be monitored and acted upon immediately. TSCM shall be applied.

VII. Access Control on Stand Alone and Portable Microcomputer

Access to information stand-alone and portable microcomputers on which sensitive and classified data is processed, shall be controlled and limited by means of approves access control software and/or hardware.

6.3.9 Password management

6.3.9.1 Password Security

The selection of passwords, their use and management as a primary means to control access to systems is to strictly adhere to the best practice guidelines. Passwords shall be individual and exclusive, allocated with discretion and shall not be disclosed without authorization. All personnel must treat passwords as private and highly confidential. Quality passwords with a minimum length of six characters shall be selected. Users shall change passwords on receipt and sign an undertaking to keep personal passwords confidential. Unauthorized disclosure shall be considered a breach of security and an infringement of Section 3 and 4 of the Disclosure of Official Information Act.

6.3.10 Password Administration

6.3.10.1 The designated official responsible for IT management and support within DPS shall, in writing, appoint password administrators as well as owners of master and sub-master passwords to control the allocation and amendment of passwords. Only personnel of the DPS may authorize the regeneration of forgotten/expired passwords.

6.3.10.2 Temporary passwords shall be conveyed to users in a secured manner and users shall be forced to change them immediately. A user with access to sensitive and classified data shall change his/her password at least once a month. A user with access to confidential data shall only change his/her password once every three months. The access control system shall force the user to change the password by refusing access to the system after the specified time.

6.3.10.3 Passwords transmitted over network lines as well as those stored on mainframe systems shall be encrypted.

6.3.10.4 The password, smart cards, tokens and cryptographic keys database shall be classified at least secret, encrypted and administered accordingly. Password files shall be stored separately from the main application system data.

6.3.10.5 Audit trails shall be used in all SECRET and TOP SECRET transactions. The audit trail shall indicate which amendments have been made to passwords. The password administrator shall monitor the information at least once a month and any irregularities shall be reported thorough the normal chain of command to the System Manager and the DPS IT security structure for further investigation.

6.3.11 Workstation Security

6.3.11.1 Safeguard Hardware and Peripheral Equipment

Microcomputer shall be located in a physically protected environment where access control measures are in place and applied consistently. All users of PCs, laptops or workstations are to ensure that appropriate and approved password protected "Screen Saver" software is loaded on their PC's, laptops or workstations and activated when the PC, laptop or workstation is secured by a key lock or an equivalent device when not in use, or that the PC, laptop or workstation is secured by a key lock or an equivalent device when not in use. Microcomputers shall only be used for official DPS purposes. Any movement of hardware between the DPS's locations is to be strictly controlled by authorized personnel.

6.3.11.2 Safeguarding Portable Microcomputers

i. All portable microcomputers e.g Laptops, Notebooks, Palmtops etc shall be equipped with an access control capability that meets approved security standards. An official anti-virus package shall be installed and updated regularly.
ii. Portable microcomputers of the DPS shall not be linked to modems or equipped with fax cards without approval of the HOD responsible for IT security.
iii. Only approved software shall be loaded on portable microcomputer.

iv. Removal control measures shall be loaded on portable microcomputers.

v. Before undertaking foreign trip, user shall provide written confirmation that no unauthorized information is stored on the portable microcomputer.

6.3.11.3 Safeguard Stand-alone Microcomputers

i. Access to stand alone microcomputers on which sensitive and classified data is processed, shall be controlled and limited by means of approved access control software and/or hardware. Active sessions shall be terminated when leaving the workstation or a password protected screen saver shall be installed.

ii. Stand-alone microcomputers on which sensitive and security classified data is processed shall only have removable media that are secured when not in use.

iii. The menu system shall be configured to discourage use of the operating system command shell directly.

iv. Under no circumstances shall anyone other than authorized IM structure maintenance personnel be allowed to change any of the hardware or the complementary metal-oxide semi-conduct (CMOS) settings. Written approval of the System Manager shall be obtained before any changes to the CMOS settings are implemented. Ownership of equipment shall be embedded in the CMOS setting.

6.3.12 Hardware Modification and Repair of Microcomputers.

i. The upgrading of microcomputer hardware shall be approved by the System Manager.

ii. Only approved maintenance personnel with valid security clearances shall be approached for the repair or modification of microcomputers. The repair/modification of microcomputers with hard discs shall be performed under the supervision of a computer knowledgeable member of DPS.

iii. If the hard disc is to be removed from the DPS's premises, it shall be formatted before being repaired, by overwriting it eight times with binary ones and zeroes. If a hard disc cannot be accessed, it shall be presented to IT management and support structure to be physically destroyed.

iv. When microcomputers have been repaired, the hardware shall correspond with the configuration shall be reported to the System Manager for further investigation.
v. Spare parts removed during repairs shall be disposed of according to the prescribed disposal procedures.

6.3.13 Safeguarding of Software

The acquisition, utility, storage access control and safeguarding of microcomputer software shall be done in accordance with applicable policies and procedures on procurement and software management.

6.3.14 Safeguarding of Information, and data

6.3.14.1 Sanitizing

i. Temporary files on user's PCs and laptops are to be deleted regularly to prevent possible misuse by possible unauthorized users.
ii. If no longer required, the previous contents of any re-used media shall be erased.
iii. The content of magnetic media containing no sensitive information shall be erased by degaussing or overwriting it at least three times, and laser printer drums by printing at least three full pages of unclassified text. Hard discs and media containing sensitive information shall be overwriting them eight times with binary ones and zeroes.

6.3.14.2 Protection and Backup

i. All users of information systems whose job function requires them to create or amend data files, must save their work on the system regularly in accordance with best practice, to prevent corruption or loss through system or power malfunction.
ii. An Uninterruptible Power supply is to be installed to ensure the continuity of services during power outages.
iii. In order to protect magnetic media against incidental and/or deliberate damage, the supplier's utilization and storage specifications shall be adhered to, and the media shall be protected against electromagnetic radiation.

iv. In order to prevent damage to the hard disc components, care shall be taken that the hard disc is safeguarded in accordance with specifications before microcomputers are moved.

v. Information system owners must ensure that adequate backup and system recovery procedures are in place. Backup media shall be stored at a geographically separate location in fireproof cabinets. It is the responsibility of the user of laptops or portable computer to ensure that the computer is back-up on regular basis. Supervisory personnel must ensure the safeguards are in place to protect the integrity of data files during the recovery and restoration of data files, especially where such files may replace more recent files.

vi. The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered, especially where proprietary formats are involved.

6.3.14.3 Disposal

Disposal of any data or data media shall be done in accordance with the prescribed standards.

6.3.15 Off-site Usage

- Line Management must authorize the issue of portable computers or Off-site computer usage. Usage is restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, especially responsibility for the security of information held on such devices.
- Personnel using business centers to work on the DPS's business are responsible for ensuring the security and subsequent removal and deletion of any information entered into the business center systems.

6.3.16 Monitoring of Home Terminals

- The authorized allocation of home terminals to members shall be discouraged. It shall only be authorized in exceptional cases with a written motivation as well as a security plan provided by the System Manager and the authorization of the designated official responsible for IT security. Members who use home terminals shall sign a form of compliance that the

security policy in respect of home terminals shall be complied with. The System Manager shall keep record of all home terminals within his/her area of responsibility.

- Before any such authorization can be granted, the physical and personnel security prescriptions shall be complied with. Users shall at least have a valid security clearance.

Control measures and procedures shall ensure that:

i. No access is given to any of the production areas/centers. Applications for such access shall be fully motivated and will only be approved in exceptional cases by the designated official responsible for IT management and support.
ii. Only approved dial-back modems are used for authentication.
iii. The utilization of the equipment is monitored continually in terms of its essentiality, as well as the application of the prescribed security measures.
iv. Record is kept of the placement and withdrawal of home terminals.
v. Access is limited to only that data which is absolutely essential to the performance of the user's job and a unique security profile is drawn up for this purpose. If any additional access is required for any system(s) other than the access that was originally approved, the designated official of DPS responsible for IT security shall authorize such a request and the employee's security profile for IT security shall authorize such a request and the employee's security profile shall be adapted accordingly.
vi. Access to the system is only gained through a single point of entry port (network port) and by means of a secured firewall.
vii. Re-motivation, re-application, re-assessment and re-quests are done every six months as well as in the case of transfers or relocations.
viii. Special authorization is obtained for removable media.

6.3.17 Utilization of Private PC's on DPS Premises.

i. Written approval shall be obtained from the relevant System Manager to use a private PC on the premises.

ii. No private computer with a modem shall be allowed on the DPS premises for any reason.

iii. A PC register shall be established by the responsible supervisor of each structure of DPS who has control over computer containing full personal particulars of the person as well as details of the computer eg Make, serial no. tapes and software used.

iv. A private PC shall be considered shall be considered government property during use on the DPS premises. All policies, guidelines and standard operating procedures shall apply to the PC.

v. Before a private PC can be brought into and /or removed from the premises of DPS, it shall be verified that no classified information is stored on the hard disc. The removal of a private PC from the DPS premises shall be authorized by the System Manager.

vi. The designated official of DPS responsible for IT security shall be notified of the private PCs used on the DPS premises

vii. Any unauthorized private PCs on the DPS premises shall be confiscated during monitoring actions.

6.3.18 Disaster Recovery Plan

i. DPS shall have a documented and updated disaster recovery plan and emergency procedures for each system that has to be recovered in the event of emergency. This will be approved by the supervisor who has been assigned control of the respective systems is the owner of the respective disaster recovery plans. These plans shall be documented and shall at a minimum, adequately cover priorities, preventative measures and procedures.

ii. Disaster recovery plans and procedures shall be tested, evaluated with regard to effectiveness and updated at least once a year. A variety of test techniques shall be used to ensure that the plans will be effective in an emergency situation e.g paper testing of the various scenarios, simulations, technical recovery testing and live testing. The designated official of a DPS responsible for IT management and support and of IT security shall be notified timeously of any live disaster recovery exercises. No exercise with regard to

the mainframe systems and bigger distributed systems shall take place without appropriate authorization.

iii. A disaster recovery plan is a blueprint of an organization's weaknesses and it is therefore a document that shall be distributed on a need –to know basis. The recovery plan shall at least be classified CONFIDENTIAL.

iv. Security responsibilities shall be identified and allocated. The conditions for activating the plan shall be clearly stated.

v. Any unique technology shall, where possible, be backed up for use in a disaster situation. Original software shall be available for the operating and application system.

6.3.19 Electronic Mail

i. Sensitive and classified information shall not be transmitted via E-mail unless authorized by the appropriate authority and encrypted with approved encryption devices.

ii. Logical access to the DPS E-mail system shall be restricted to authorized users and a unique password shall be used to validate a user's identity before access to the system can be gained.

iii. DPS E-mail system shall not be used for unlawful activities, commercial purposes not under the auspices of the DPS, personal financial gain, messages that might be offensive or discriminating and / or other uses that violate this or other DPS policies.

iv. E-mail users of the DPS shall not employ a false identity when using the E-mail system or someone else's computer to send E-mails.

v. E-mail services shall not be used for purpose that could reasonably be expected to cause excessive strain on any computing facility or unwarranted interference with other user's use of E-mail services.

vi. All E-mail software that is installed and /or upgraded shall be appropriately authorized (certified and accredited) by the DAA of DPS before installation proceeds.

vii. Access to the DPS's Email system shall be revoked after termination of employment.

viii. Data retention periods for E-mail must be established to meet legal and business requirements and must be adhered to by all employees.

6.3.20 Internet connection

An internet workstation linked to an internal network allows for the internal network. Persons responsible for setting up internet access are to ensure that the DPS's network is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall. Note must be taken that firewalls are not foolproof and are open to hacking attempts.

The majority of internet traffic is not encrypted, allowing for e-mail, passwords and file transfer to be monitored and captured, using readily available software. The communication lines (fixed or telephone) are also subjected to tapping and can therefore not be trusted, as they are not encrypted. The negligent, ignorant or malicious use of the internet can result in abuse of funds, embarrassment to the DPS, or denial of services.

I. Internet connections shall be implemented by means of air wall concept (stand-alone computer /network), not connected to any sensitive network of DPS. Access to the internet shall as far as possible not be allowed via a telephone (PBX) line –data lines shall be used to establish the link. A modem shall under no circumstances be connected to PC linked to the DPS's internal network to enable access to the internet. Access. Access control shall be exercised by means of approved firewalls for networks. File compression shall be used where possible.
II. The internet shall not be used for classified or sensitive information, internal communication to the DPS or as a substitute for the existing communication infrastructure.
III. Additional precautions must be taken when downloading information and files from the internet to safeguard against malicious code. Material which is inappropriate, illegal, and offensive or which jeopardizes security may not be downloaded.
IV. The downloading of commercial software is strictly prohibited, unless appropriately approved by IT security structure. An approved anti-virus package shall be installed on every internet computer and regularly updated. All software to be used on the DPS's computers shall only be installed by IT management and support structure, following all licensing agreements and procedures. The system administration staff will inspect the computers periodically to verify that only approved and licensed software has been installed.

V. Computer files received from unknown senders are to be deleted without being opened. This applies to unsolicited, unfamiliar or any form of bogus e-mail.

VI. A sound IP address scheme shall be developed, documented and implemented on every participating Internet Protocol (IP) network of DPS.

VII. Activation of TCP\IP services shall be implemented taking into consideration the implied security weakness related to each particular service, e.g Telnet sessions. The allocated abilities shall be re-evaluated every six months by the designated authority.

VIII. No official information may be stored on an Internet workstation.

6.3.21 Misuse

Misuse of access to the electronic resources and facilities of an DPS such as the use of personal software or equipment on a DPS's workstations or network, or of internet access, shall result in disciplinary action. Other prohibitions on the utilization of Internet facilities within DPS include the following:

i. Illegal, unlawful or immoral usage. Example of this would be the intentionally transmitting, communicating or accessing of pornographic or sexually explicit material, images texts or other offensive material.
ii. Use the networks for commercial or partisan political purposes. This includes using the network traffic for any purpose unless engaged in authorized network administrative duties.
iii. Attempt to circumvent or subvert systems or network security measures.
iv. Intercept network traffic for any purpose unless engaged in authorized network administrative duties.
v. Make or use illegal copies of software or other media on which copyright exists, store such as copies on DPS systems, or transmit them over DPS owned networks.
vi. The Internet shall not be used to store or process classified and sensitive information such as communication between employees; excessive private use that influences the productivity of the system for others, or that results in additional financial expenditure, without appropriate approval.

6.3.22 Disposal of Computer-Related Articles

6.3.22.1 Disposal of hardware.

i. Equipment owned by DPS may only be disposed of by authorized personnel who have ensured that the relevant security risks have been mitigated.
ii. Any third party used for external disposal of the DPS obsolete equipment and material must be able to administrate compliance with this DPS's Information Security Policies and also, where appropriate, provide a SLA which documents the performance expected and the remedies available in case of non compliance. SITA is strategically positioned to take charge of this issue.
iii. Data shall be removed from any hard disc/storage device before it is disposed of/destroyed. The hard discs/storage device shall be formatted by overwriting it eight times with binary zeroes and binary ones or by using an approved utility program that overwrites all the data with zeroes. If a hard disc/storage device containing sensitive on formation is damaged and cannot be accessed electronically, it shall be stored in a safe place until it can be destroyed in accordance with the prescribed procedures.
iv. Cryptographic equipment may not be disposed of and shall only be removed by the cryptographic/crypto custodian for safeguarding.

6.3.22.2 Disposal of records and information

The retention, storage, handling and disposal of computer related records and information shall be managed in accordance with the applicable policies of the DPS on records management and information security. A retention schedule shall be drawn up identifying essential record types and the period of time for which they will be retained. Appropriate controls shall be implemented to protect essential records from loss, destruction and falsification.

6.3.22.3 Disposal of data

When data that forms part of a transversal system is disposed of, the System Manager shall obtain written comments from other users or System Managers in respect of the impact of the disposal on their systems. The request to dispose of

transversal systems shall be submitted to the Department of State Expenditure for authorization. Where possible, outdated technology shall also be archived in order to access archived information.

6.3.23 Incident Management

6.3.23.1 Theft or Loss

If the any IT asset is lost or stolen it must be reported to the Local Police immediately. The police report should include the serial number for the lost computer. A copy of the police report must be sent to the Deputy Director: MISS, lost control section and IT manager within 48 hours of the discovery of the loss. Failure to secure and submit a police report may result in personal liability for replacement cost.

6.3.24 Personnel Security

6.3.24.1 Recruitment and Security Screening

i. Consultants/contractors/third parties located on-site for any period of time are also subjected to the requirements of this policy and standards and shall be managed like any other system user of the DPS.
ii. Before an ITS user/contractor is appointed, the applicant shall meet the minimum security requirements for the post. In the case of external contractors, the following shall be adhered to:

- Terms and conditions of Employment of all state organizations shall include requirements for compliance with Information Security.
- All external suppliers who are contracted to supply services to the DPS appropriate summary of the Information Security policies must be formally delivered to any such suppliers, prior to any supply of services.
- Non-disclosure agreements must be used in all situations where the classified as Proprietary (or above).
- Any Information Security incidents resulting from non-compliance will result in immediate disciplinary action.

iii. All IT related positions shall be evaluated and assigned a sensitivity level. Appropriate vetting of members and contractors at the assigned level of sensitivity / classification of each system and at prescribed intervals shall be conducted for all members before filling these positions. Programmers and mainframe computer System Managers shall prescribe security clearance. The security classification of the information or system shall also determine the level of clearance needed for contractors or any other person in terms of DPS vetting policy prior to their being allowed to participate in the design, operation or maintenance of IT systems, or to access the DPS systems.

iv. Before an ITS user/contractor is transferred to a post with a higher security grading, the member shall already have the appropriate security clearance. If this is not possible, the designated official who has been assigned control over the system (system owner) shall accept written responsibility for the utilization of member or contractor for perform a specific job.

v. The re-clearance of IT systems user/contractors in posts with high security grading shall be done in accordance with prescribed procedures. An employee whose clearance has expired and whose application for the renewal of the clearance has already been received by the IT security structure, may be allowed access to classified information up to the same level of his/her expired security clearance for a maximum period of three months. The system owner shall accept responsibility for the member to perform a specific job.

vi. Access to networks/data centers shall automatically be terminated on expiry of an employee's/contractor's security clearance. In order to prevent denial of services/access, users shall timeously apply for a re-clearance.

6.3.24.2 Resignations

- Key personnel/users in a high-risk environment shall, when they state their intention to resign, be transferred to a lower risk environment. They shall not have access to sensitive and classified information (particularly secret or top secret) for at least the last 30 days before they leave. Backup actions shall be in place in this regard and an audit trail shall be instituted on their actions

- The clearing-out administration for the system users/contractors shall provide for the following:
  - ❖ Completion of the Disclosure of Official information Act.
  - ❖ Change of passwords
  - ❖ Immediate cancellation of access to systems.
  - ❖ Removal from the system(s).
  - ❖ Submission all computer equipment.
  - ❖ Submission of all official documentation.
  - ❖ Information of all people concerned of the member's termination of service.
- Before the computer equipment of a user who has resigned is handed over to another user, the System/LAN Manger shall certify that there is no classified information on the computer.

6.3.25 Information Technology Security Training

- Training shall be provided to effectively and efficiently apply IT security. Security consciousness shall continually be promoted amongst personnel and should be followed up by means of formal training programs.
- DPS need to ensure that all employees are fully aware of their legal responsibilities must be included within key staff documentation such as terms and conditions of Employment and the Organization Code of Conduct.
- DPS must prepare guidelines to ensure that all employees are aware of the key aspects of Computer Misuse legislation (or its equivalent), in so far as these requirements impact on their duties.

6.3.25.2 Key Personnel

Key personnel shall be identified and backup personnel shall be trained. Contractors shall not be appointed in key posts or employed as project officers.

6.3.26 Protection of Copyright

Materials obtained or copied on the internet may be subjected laws that govern the making of reproductions of works on which copyright exists. A work protected by copyright may not be copied without permission of the copyright owner unless the proposed use falls within the definition of "Fair Use". Members are responsible for compliance with the Copyright

Act, 1978 (Act No 98 of 1978), and any amendments thereof and all international laws governing copyright. The manner of collecting overt information shall, as far as possible, allow for acknowledgement of sources. When using overt information, acknowledgement of the source shall include the following basic bibliographical information: Author, Title (if an article, title of both periodical and article) and date of publication.

7. Responsibility and Obligations

- The DPS systems are to be managed by a suitably qualified systems administrator who is responsible for overseeing the day to day running and security of the systems. The designated Administrator must be fully trained and have adequate experience in the wide range of systems and platforms used by DPS and must be acknowledgeable in the range of Information Security risks which need to be managed.
- IT directorate shall take full responsibility of ensuring that all the services rendered are DPS business enabling.
- It is GITOC's responsibility for the existence/relevancy and applicability of MIOS standards in all DPS Information systems and IT projects.
- It is Users, IT Personnel and all Stakeholders' responsibility to ensure compliance with this policy.
- Users/Complainants are to ensure that all their IT service requests are referenced with a number from help desk.
- IT personnel must avoid at all costs attending to any call without any reference number, as this may lay negative impact during time of assessment.
- IT a responsibility of users entrusted with DPS IT assets ownership (temporary) to ensure that they are secured and are in good condition.
- Departmental HOD shall ensure compliance with MIOS in the project procedure approval for the department. The MIOS shall be used in the audit and review of every project of a department.
- The HOD shall ensure that the acquisition, management and use of IT by the department improve the following:
    i. Direct or indirect service delivery to the public, including, but not limited to, equal access by the public to services delivered by DPS.

ii. The productivity of the department.
iii. The cost-effective of the DPS.

8. I.T Operational Support Guidelines

8.1 1st Line Support

- Any fault/request of IT service shall be reported to the IT help desk on this number (018) 388 1111, where a unique reference number shall be issued to a complainant / concerned user.
- Service desk operator shall then assign a call/reported problem to the respective IT personnel for his/her attention.
- A reported call shall by any means be accepted by respective IT personnel and be attended to, in accordance to what is entailed in the SLA document.
- User/complainant shall be updated from time to time about the status of his /her call or request for service.
- IT Service Manager/supervisor shall monitor all reported calls/requests thereby ensuring user or customer's service satisfaction.
- Escalated calls shall be managed in accordance to what is entailed in the SLA document.

9. Dispute Resolution

- Violation of this policy may result in disciplinary action in accordance with DPS disciplinary policy and procedures.
- Should it come to the attention of System Manager that omissions/negligence or actions of an employee are endangered the security of the system, he/she shall suspend the relevant employee's access privileges in accordance with the gravity of the actions concerned and report the negligence/actions/omissions to the IT security and/or counterintelligence structure through the normal management channels.

10. Monitoring and Evaluation

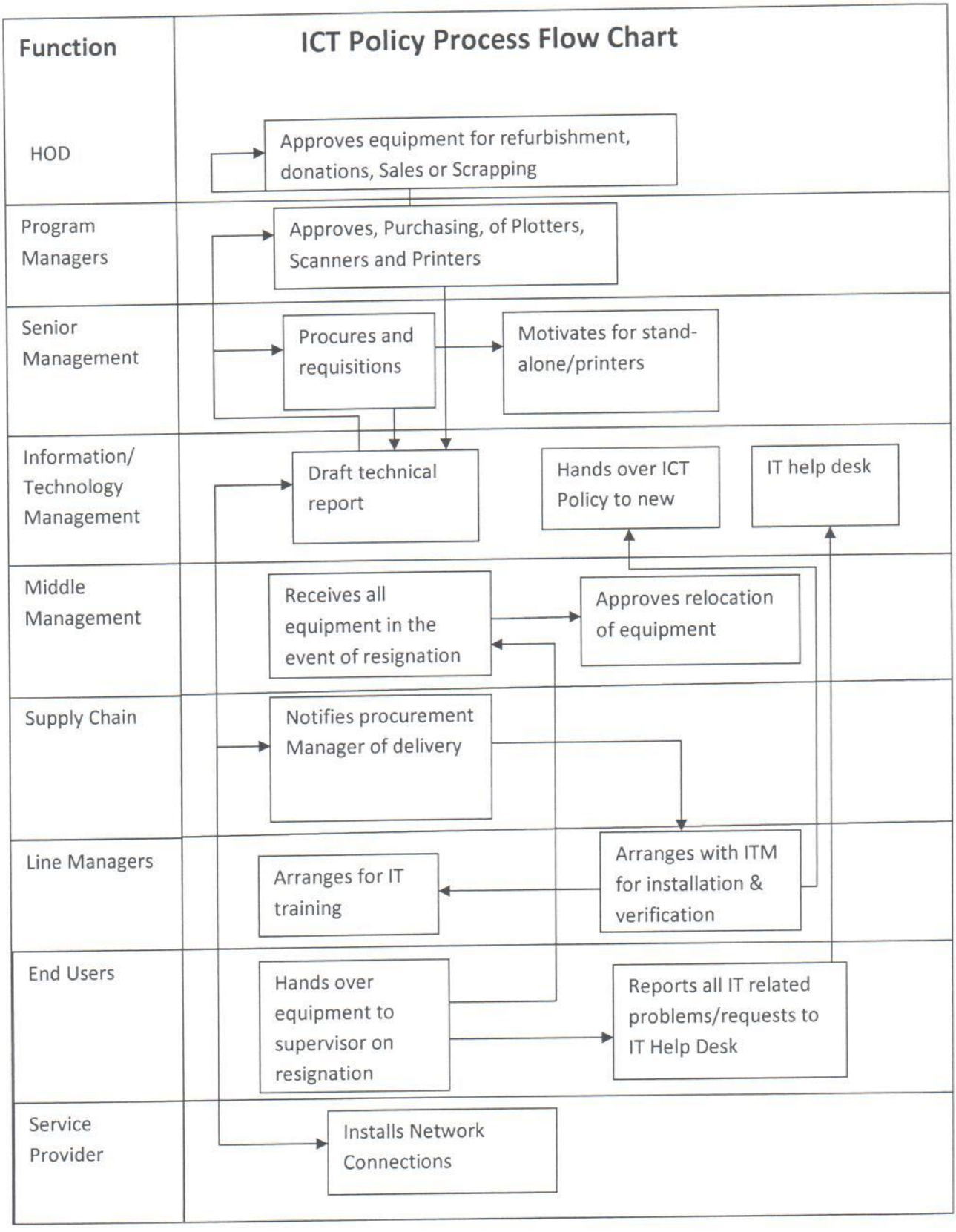
- Operating Systems must be regularly monitored and all required 'housekeeping' routines adhered to.
- Operational staff shall maintain an audit log of all operational activities. Operational audit logs are to be reviewed regularly by trained staff and discrepancies reported to the owner of the information system.
- DPS systems are to be monitored and evaluated timeously to ensure the relevancy of technology mapping to business requirements.
- Compliance with the security requirements shall be monitored and audited by the IT security structure of DPS.

11. Related Policies

Supply Chain Policy
Human Resource Management Policy
MISS
Records Management
Department of Finance IT Policy
Public Finance Management Policy
Risk Management Policy

11.1 Policy Drivers

- HOD
- Program Managers (Chief directors)
- Senior Management
- Middle Management
- Supply Chain
- Line Managers
- End Users
- Service Providers (Finance IT)


Function
ICT Policy Process Flow Chart
HOD
Approves equipment for refurbishment, donations, Sales or Scrapping
Program Managers
Approves, Purchasing, of Plotters, Scanners and Printers
Senior Management
Procures and requisitions
Motivates for stand-alone/printers
Information/ Technology Management
Draft technical report
Hands over ICT Policy to new
IT help desk
Middle Management
Receives all equipment in the event of resignation
Approves relocation of equipment
Supply Chain
Notifies procurement Manager of delivery
Line Managers
Arranges for IT training
Arranges with ITM for installation & verification
End Users
Hands over equipment to supervisor on resignation
Reports all IT related problems/requests to IT Help Desk
Service Provider
Installs Network Connections

11.2 Description of Procedure

Service Providers:

- Installs network connections.

End User:

- Hands over equipment to supervisor on resignation.
- Reports all IT related problems/requests to IT Help Desk.

Line Managers:

- Arranges for IT training
- Arranges with ITM for installation & verification.

Supply Chain:

- Notifies procurement Manager of delivery.

Middle Management:

- Receives all equipment in the event of resignation.
- Approves relocation of equipment.

IT/S Management:

- Draft technical report.
- Hands over ICT Policy to new.
- IT help desk.

Senior Management:

- Procures and requisitions.
- Motivates for stand-alone/printers.

Program Managers:

- Approves, Purchasing, of Plotters, Scanners and Printers.

HOD:

- Approves equipment for refurbishment, donations, Sales or Scrapping.

Approved / ~~Not Approved~~

.....

Mr. B. Mahlakoleng

Acting Head of Department