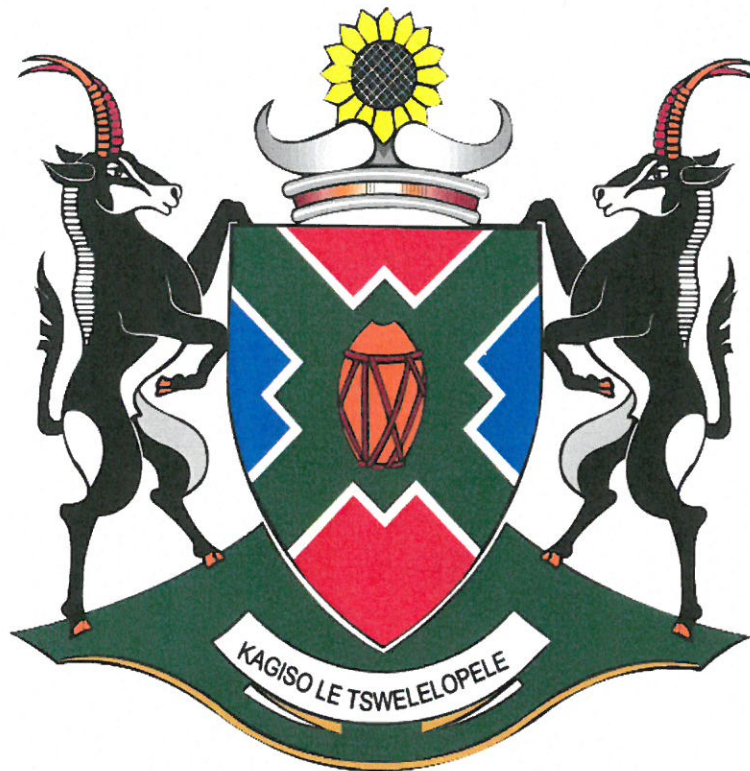


DEPARTMENT OF COMMUNITY SAFETY & TRANSPORT MANAGEMENT



GOVERNANCE AND MANAGEMENT OF ICT FRAMEWORK

GMICTF—VERSION 1.2



### Document Details

<b>Author</b>	Directorate Strategic Support Services
<b>Department</b>	Community Safety and Transport Management
<b>Division Name</b>	ICT Management
<b>Document Name</b>	Governance and Management of ICT Framework
<b>Sensitivity</b>	Internal Use Only
<b>Effective Date</b>	<HoD's signature>
<b>Created Date</b>	30-06-2013
<b>Version Date</b>	<HoD's signature>
<b>Version</b>	GMICTF-VERSION 1.2

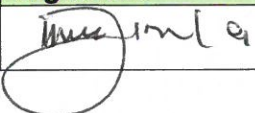
### Change Record

Modified Date	Author	Version	Description of Changes
26-09-2014	Directorate Strategic Support Services	1.1	Departmental Business Change
31-03-2016	Directorate Strategic Support Services	1.2	Annual review

### Stakeholder Sign-Off

Name	Position	Signature	Date
Mr S. Matlhako	Departmental Information Technology Officer & Director Strategic Support		14/07/2016
Ms K. Phatudi	Strategic Committee Chairperson & Governance Champion		14/07/2016
Ms M.G. Mothibedi	Departmental Risk Management Officer		14/07/2016
Mr S. Setlhare	Acting Director Legal Services		14/07/2016

### Records Management Sign-Off

Name	Position	Signature	Date
Mr E. Jimla	Records Manager		14/07/2016

## Glossary of Terms

<b>CGICTPF</b>	Corporate Governance of ICT Policy Framework
<b>Corporate Governance</b>	<p>"...The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly." (IT Governance Institute: ISACA [CGEIT] Glossary: 5 as amended)</p> <p>Procedures and processes according to which an organisation is directed and controlled. (Glossary of Statistical Terms – Organisation of Economic and Co-operation Development <a href="http://www.oecd.org">www.oecd.org</a>)</p>
<b>Corporate Governance of ICT (CGICT)</b>	<p>The system by which the current and future use of ICT is directed and controlled.</p> <p>Corporate governance of ICT involves evaluating and directing the use of ICT to support the organisation, and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organisation. (ISO/IEC 38500: 2008: 3)</p>
<b>DPSA</b>	Department of Public Service and Administration
<b>Executive Authority</b>	<p>(a) the Office of a Premier or a provincial government component within a Premier's portfolio, means the Premier of that province; and</p> <p>(b) a provincial department or a provincial government component within an Executive Council portfolio, means the member of the Executive Council responsible for such portfolio;</p>
<b>Executive Management</b>	The Executive Management of the Department and could include the Head of Department, Deputy Directors-General (DDGs) /Executive Management of the Department. This normally constitutes the Executive Committee of the Department and should include the GITO.
<b>GICT</b>	Governance of ICT
<b>GITO</b>	Government Information Technology Officer (Cabinet Memorandum 38(a) of 2000)
<b>GITOC</b>	Government Information Technology Officer's Council (Cabinet Memorandum 38(a) of 2000)
<b>Governance Champion</b>	The Senior Manager in the department who is responsible to drive Corporate Governance of and Governance of ICT.
<b>Governance of ICT</b>	<p>The effective and efficient management of IT resources to facilitate the achievement of company strategic objectives. (King III Code: 2009: 52)</p> <p>Is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's</p>

	strategy and objectives (ITGI 2005) The system by which the current and future use of IT is directed and Controlled.
<b>Department / dcs&amp;tm</b>	The Department of Human Settlements, Public Safety and Liaison (Public Branch)
<b>HoD</b>	Head of Department or Organisational Component as per the PSA
<b>ICT</b>	Information and Communications Technology, also referred to as IT
<b>ISO/IEC 38500</b>	International Standard on Corporate Governance of ICT (ISO/IEC WD 38500: 2008: 1)
<b>IT</b>	Information Technology , also referred to as ICT
<b>MISS</b>	Minimum Information Security Standards
<b>MIOS</b>	Minimum Interoperability Standards

## TABLE OF CONTENTS

1. Introduction .....	1
2. Regulatory and Guidance Framework.....	1
3. Scope and Application .....	1
4. Purpose.....	1
5. Governance and Management.....	2
6. ICT Strategy.....	2
7. ICT Management .....	3
8. ICT Change Management.....	4
9. ICT Security .....	4
10. Ownership and Custodianship of Hardware, Software and Data .....	6
11. ICT Contingencies .....	6
12. ICT Procurement Framework.....	7
13. Utilisation of ICT Assets and Resources .....	9
14. ICT Support.....	11
15. Monitoring and Evaluation.....	11
16. Review of the Framework .....	12
17. Approval.....	12

## **1. Introduction**

The Department recognises the significant advantages of using technology to enable its business for the harnessing of the mandated service delivery. There are standing issues surrounding the governance and management of Information and Communication Technologies within the department as reflected in the successive Auditor - General Reports.

Expenditure on IT can represent a significant proportion of an organization's expenditure of financial and human resources. However, a return on this investment is often not realized fully and the adverse effects on organizations can be significant. The main reasons for these negative outcomes are the emphasis on the technical, financial and scheduling aspects of IT activities rather than emphasis on the whole business context of IT use.

This framework is essential in addressing governance and management of ICT within the department.

## **2. Regulatory and Guidance Framework**

The following documents inform the development of this framework

- Public Service Act and Regulations (as amended)
- Public Finance Management Act
- State Information Technology Agency Act and Regulations (as amended)
- The Corporate Governance of ICT Framework
- CGICT Assessment Standard
- MISS
- MIOS
- Treasury Regulation 12

## **3. Scope and Application**

The framework is applicable to all employees within dcs&tm utilising the department's ICT resources and facilities in pursuing departmental goals and strategic objectives.

## **4. Purpose**

This framework has been established in the Department to:

- 4.1. provide guidelines for the conditions of acceptable and appropriate use of ICT resources installed and configured for use;
- 4.2. provide standards for users in the management and use of ICT resources;
- 4.3. ensure the confidentiality, integrity and availability of data and ICT resources;

## **5. Governance and Management**

**5.1** The following governance and management of ICT committees and other key stakeholders are established to deal with ICT matters:

### **5.1.1** *ICT Strategic Committee –*

This committee shall conceptualise and oversee the Corporate Governance of ICT, Governance of ICT and the strategic alignment of ICT to the core business of the department.

### **5.1.2** *ICT Steering Committee –*

This committee shall coordinate and oversee the planning, implementation and execution of the Corporate Governance of ICT, Governance of ICT, and strategic alignment of ICT to the business of the department and monitor the implementation thereof.

### **5.1.3** *ICT Operational Committee –*

This committee shall keep track of the day-to-day ICT service management elements as well as reporting on a monthly basis to the ICT Steering Committee on the implementation of the ICT implementation plan.

### **5.1.4** *Governance Champion-*

Governance Champion shall drive Corporate Governance of and Governance of ICT and. Create enabling environment for CGICT and GICT

### **5.1.5** *Departmental Information Technology Officer (DITO)-*

Alignment and implementation of business and ICT strategies, conformance and performance measurement and ensure ICT service delivery. Ensure compliance to the ICT legislative prescripts.

**5.2** The composition, roles, responsibilities and terms of reference of these committees and other key stakeholders are set out in the departmental CGICT Policy and Charter.

## **6. ICT Strategy**

**6.1** The ICT Strategic Committee shall be responsible for the development of a departmental ICT Strategic Plan that is aligned to the business processes and requirements of the department.

**6.2** The ICT Strategic Plan should cover at least the Medium term Expenditure Framework or the Medium Term Strategic Framework (MTSF), which must be aligned to the 5 year electoral cycle;

**6.3** The ICT Strategic Plan shall be updated accordingly should business or technology changes present risks or opportunities that should be reflected in the plan.

**6.4** The ICT Strategic Plan shall contain at least:

**6.4.1** A clear definition of the current business processes and requirements of the Department;

**6.4.2** Statements of expected changes in the business and structure of the Department for three years period started from;

**6.4.3** Descriptions of the capabilities of the existing ICT infrastructure;

**6.4.4** Evaluation of the gaps between the current and future business ICT requirements of

- the Department and the capabilities of the existing ICT infrastructure;
- 6.4.5 Proposals to eliminate the gaps referred to in (6.4.4) above;
- 6.4.6 Documentation of new technologies, their likely impact on the business of the Department and their expected cost.

6.5 The ICT Strategic Plan shall be reviewed approved by the Head of Department prior to **31 March 2020**.

## 7. ICT Management

7.1 The ICT Steering Committee shall coordinate and oversee the planning, implementation and execution of the Corporate Governance of ICT, Governance ICT, and strategic alignment of ICT to the business of the department.

7.2 The ICT Steering Committee shall monitor the implementation of Corporate Governance of ICT, Governance of ICT, and strategic alignment of ICT to the business of the department.

7.3 Management of ICT shall be governed by all the approved ICT policies and prescripts.

### **Evaluate by:**

- Coordinating the development/review of CGICT Policy.
- Coordinating the development of ICT Strategic Plan, Implementation Plan, ICT Budget Plan, ICT Security Plan, and Change Management Plan based on direction received from the ICT Strategic Committee.
- Determining, prioritizing and recommending Plans, Policies, Strategies, Resource/Capacity requirements, portfolios of ICT projects and risk management to ICT Strategic Committee and/or HoD.
- Overseeing the identification of the ICT prescriptive environment.

### **Direct:**

- The implementation of approved plans, policies, strategies, resource/capacity requirements, risk management, benefits realization, portfolios of ICT projects, internal and external audits.
- The monitoring criteria and related reporting requirements and processes for conformance, performance and assurance.
- All ICT related decisions that may have an impact on the business operations and culture of the department that is escalated to the Committee.
- The change management requirements for the implementation of CGICT and report to Strategic Committee.
- The preparation and presentation of a Three/Five-year rolling ICT Strategic Plan by **31 March** of each year;
- The implementation of new hardware, operating systems and application software and obtain the recommendations of ICT procurement agencies, where ICT requirements change.
- The recommended budget for specific and transversal ICT systems and services.

### **Monitor:**

- Conformance to all ICT Policies and Prescript, Performance and Reporting of ICT operations to ICT Strategic Committee.



- The procurement of all ICT goods and services, transversal as well as specific.
- The maintenance and control of all ICT systems, which shall include hardware, operating systems and application software.

**7.4** Each transversal system shall have;

The system controller shall ensure that the system is used according to National and Provincial standards and to resolve any exceptions arising from the use of the system.

**8. ICT Change Management**

**8.1** All changes to hardware, operating systems or application software shall be requested in writing by the user of the system and approved, in writing, by the:

- 8.1.1** Program manager of the respective directorate;
- 8.1.2** ICT representative from the directorate where the change is to be made; and
- 8.1.3** Manager of the ICT component.
- 8.1.4** And / or Request for Change Committee / Steering Committee.

**8.2** All changes to hardware, operating systems or application software shall be:

- 8.2.1** Consistent with National and Provincial standards, where such standards exist; and
- 8.2.2** Tested prior to implementation.

**8.3** Where significant changes are made to any system that, if not made successfully, may cause the system to fail or behave unreliably, the system shall be backed up prior to the change being made. Furthermore, the reliability of restoring from the back up shall be tested prior to implementation of the change.

**8.4** Changes to hardware, operating systems or application software that do not comply with this policy shall not be made.

**8.5** All ICT related projects shall follow the processes as outlined in the approved ICT Portfolio Management Framework.

**9. ICT Security**

**9.1** All ICT systems shall have logical and physical security that is appropriate to the structure of the system concerned, the users of the systems and the confidentiality of the data contained on the systems. Where single systems have multiple levels of information security classifications then the highest level of security clearance shall be required to access all of the application software and data on the system;

**9.2** The risks associated with loss of data or confidentiality (e.g. backups) shall be assessed at least quarterly;

**9.3** Logical and physical security risks shall be assessed at least quarterly, and weaknesses identified together with appropriate recommendations shall be made to the Manager of the ICT Component/Unit;

- 9.4** All users and managers of ICT systems shall formally acknowledge their responsibility for security and maintenance of confidentiality by duly signing an agreement to this effect;
- 9.5** All ICT equipments shall have appropriate physical security
- 9.5.1** In the case of servers and shared systems this includes maintaining the equipment:
- 9.5.1.1** In a locked environment;
  - 9.5.1.2** Under conditions that provide appropriate detection and control of fire, smoke or water damage. Where other risks may exist, these should be documented and appropriate counter-measures implemented.
- 9.5.2** In the case of portable equipment this includes:
- Provision of portable security devices (e.g. locks);
- 9.5.3** Due to the inherent unreliability of storage media, only copies of data may be stored on external portable storage (e.g. flash disks, CD's, DVD's etc);
- 9.5.4** Where appropriate physical security is not / cannot be provided, then this fact, together with the implications, should be documented and reported to the Manager of the ICT Component/Unit for appropriate action.
- 9.6** All ICT equipment shall have appropriate logical security
- 9.6.1** In the case of servers and shared systems this includes:
- 9.6.1.1** Control over administrator and powerful accounts and passwords;
  - 9.6.1.2** Standards for construction and change of user accounts, passwords and privileges;
  - 9.6.1.3** Restriction of access to shared directories;
  - 9.6.1.4** Removal or disabling of guest accounts;
  - 9.6.1.5** Positive identification of all devices and users who access shared services prior to access being given;
  - 9.6.1.6** Definition of working hours and written authorisation of activities outside those hours;
  - 9.6.1.7** Logging of unexpected or unusual events and appropriate follow-up of those events.
- 9.6.2** In the case of personal computers and portable equipment this includes:
- 9.6.2.1** Control over administrator and powerful accounts and passwords;
  - 9.6.2.2** Standards for construction and change of user accounts and passwords;
  - 9.6.2.3** Removal or disabling of guest accounts;
  - 9.6.2.4** Use of screen-savers, time-outs and other utilities to prevent unauthorised use of systems;
  - 9.6.2.5** Logging of unexpected or unusual events and appropriate follow-up of those events;
  - 9.6.2.6** Consistent and automated use of passwords across multiple systems insofar as the systems supports this.
- 9.6.3** In the case of portable equipment the requirements are identical to those defined in 6.2 above but also include, in respect of laptop computers, notebook computers and Personal Digital Assistants:
- 9.6.3.1** Password protection at BIOS level; and
  - 9.6.3.2** Automatic encryption of data.

- 9.6.4 Where appropriate logical security is not / cannot be provided, then this fact, together with the implications, should be documented and reported to the Manager of the ICT Component/Unit for appropriate action.
- 9.7 User accounts, passwords and other privileges should not be disclosed or shared by anyone including authorised users.
- 9.8 In the event that an authorised user believes that another person is aware of their passwords or any other security identifier:
  - 9.8.1 These identifiers must be changed; and
  - 9.8.2 The reason for the change reported to the Departmental ICT Manager.
- 9.9 Users, as custodians of assets of the Department, are responsible for the security and integrity of:
  - 9.9.1 Data created or modified by them;
  - 9.9.2 Equipment and systems allocated to them.

## **10. Ownership and Custodianship of Hardware, Software and Data**

- 10.1 The Department is the owner of all hardware, software and data;
- 10.2 The authorised user is the custodian of all hardware, software and data;
- 10.3 All departmental data created on personal computers, including laptop and notebook computers, shall be saved on a network server.
- 10.4 The ICT Component/Unit Personnel shall maintain an ICT Asset Register, which obligation shall in no way detract from the obligation of the SCM to maintain a Departmental Asset Register;
- 10.5 ICT Component/Unit must be informed if any system or part thereof must be moved from one office to another, re-allocated to another authorised user or returned to the Department. This shall ensure that the ICT Asset Register is updated by ICT Component/Unit Personnel and the information on ICT assets is as accurate as possible. The Assets Component/Unit must also be informed, so that they are able to update the Departmental Asset Register accordingly and monitor the movement of assets between offices and officials;
- 10.6 A handing-over certificate with all the details of the system or part thereof must be signed by the previous authorised user, the new authorised user, if applicable, ICT Component/Unit Programme Manager. The duly completion of such a handing-over certificate shall transfer custodianship to the new authorised user or ICT Component/Unit, as the case may be.

## **11. ICT Contingencies**

- 11.1 ICT Component/Unit shall maintain existing systems to the best of its ability;
- 11.2 ICT Component/Unit shall ensure that all data on any server operated by the Department is secured according to acceptable back up standards;
- 11.3 ICT Component/Unit shall prepare an ICT Continuity Plan, which shall include a disaster recovery plan, which is tested at least once a year;

- 11.4** In the event of any system or part thereof being stolen/lost, the official responsible must within 48 hours, report the loss/theft to the nearest police station and the Loss Control Committee. The official should compile a report that contains a copy of the police report, statement or case number to the HOD to institute a formal investigation thereof. The equipment shall only be replaced after the loss control committee has taken a decision and it has been approved by the head of the Department. The user may be borrowed a pool computer while awaiting the approval by the head of the Department;
- 11.5** If the outcome of the investigation reveals that the stolen/lost item(s) were due to the official(s) negligence, then the official(s) shall be held responsible for the loss suffered by the state if any part of this policy or any other standing instruction has not been complied with (in accordance with Treasury Regulation 12);
- 11.6** All ICT equipment in various offices shall be in the custody of the officials to which it has been allocated to, as a result, any direct or indirect damage to this equipment due to the negligence of the official(s), the official(s) shall be held responsible for all the cost in relations to the item(s) sent for maintenance and/or repairs if any part of this policy or any other standing instruction has not been complied with (Treasury Regulation 12 refers);
- 11.7** In the event of losses the affected official(s) shall then duly inform the departmental *Loss Control Committee* who shall in turn inform the HOD to take appropriate remedial action against the official and recover all the costs the state has incurred as a result of the official's negligence.

## **12. ICT Procurement Framework**

### *General*

- 12.1** Any procurement of ICT goods and services must be channelled through the ICT Component/Unit. However, in the event of special requests made by other programmes which are not accommodated in the ICT Procurement plan, such programmes directorates shall be held responsible for the availability of funds to address that particular need.
- 12.2** Officials shall forward their requests for ICT resources in writing to ICT component for record keeping purpose.
- 12.3** A submission shall be made by ICT component outlining details of officials deemed necessary/relevant to receive any ICT resource to the Accounting Officer for approval.
- 12.4** Purchased resources shall be allocated according to the approved submission by the Accounting Officer.
- 12.5** Procurement of ICT resources and its allocation thereof shall be guided by the Supply Chain Management Processes and SITA contracts.
- 12.6** *Mobile computing equipment*

The guidelines for distribution and use of laptops are:

### ➤ Business Use Only

- A decision to provide Laptop(s) and Mobile Printer(s) shall be based upon a documented need, approval by the Program Manager, and available Departmental funds.
- Laptop(s) and Mobile Printers are intended to be used for work related purposes as productivity tools, and for research and communication. It is not intended for personal usage. Use of the Laptop(s) and Mobile Printers -should be within the standards of good judgment and common sense. These tools shall enable employees to perform urgent tasks while they are away from office premises; however no department official shall be allowed to have both a Desktop and Laptop allocated to him/her unless authorized by ICT Management.
- Since this working tools are strictly intended for work, officials should therefore not allow any third party (such as friends, relatives etc.) to use such tools.

### ➤ Software

- To the extent possible, IT technicians shall install the same software (Office Suite, email and internet, etc.) on Laptops as installed on department's Desktops. Technicians shall only install supported software(s) and no unlicensed software(s) shall be installed unless proven beyond reasonable doubt that there are challenges registered with the Licensed Software, and such an instance management has to be consulted for consent. In such an instance however the Unlicensed Software shall be installed on temporary basis until the challenge/problem is adequately dealt with.

### ➤ Criteria for Selection

Only Full time permanent employees or fixed term contract employees of the department are eligible for consideration for Laptops. Efforts shall be made to allocate Laptops to users based upon job responsibilities, demonstrated need, and approval from the Program Manager or the Delegated Official.

In general, the following groups within the department shall be considered first depending on the availability of budget.

- The MEC, HOD, Chief Directors and Directors
- Managers (from level 11 upwards) are also eligible for Mobile Tools consideration.
- Employees who travel frequently and/or not based in the office
- Employees with a daily workload that need to be completed after working hours
- The nature of employee's work
- ICT resources shall be categorised and allocated according to the appropriate ranks i.e. Senior management (incl. Executive level), Middle management and level below

- 12.7** The ICT Component/Unit shall, on merit, consider the procurement of Data Projectors and Mobile Computers per Programme, provided that these are intended for use by more than one official within the Programme and such devices are from time to time temporarily allocated from a register as the need arises e.g. Allocated Projectors for the entire Programme.

➤ **Cabling and Related Costs**

- 12.8** The ICT Component/Unit shall incur all expenditure and related costs, if the re-cabling or cabling of office(s) and/or site(s) is initiated by ICT Component/Unit. However, if the re-cabling or cabling of office(s) and/or site(s) is NOT initiated by the ICT Component/Unit Personnel, the office(s), sub-directorate(s) or directorate(s) in question; shall incur all the cabling and related costs;
- 12.9** If for one reason or the other an office(s), sub-directorate(s) or directorate(s) relocates to another building (old/new), the availability of the network points should be established before permission is granted to rent a particular building by the HoD;
- 12.10** If the lease agreement for a particular building(s), between the department and the Lesers is less than thirty six (36) calendar months, it is recommended that the cabling and the installation of data points should not be granted. This shall ensure that a thorough planning and need assessment is done before a relocation plan is approved by the HoD.

➤ **Maintenance and Repairs**

- 12.11** The ICT Component/Unit shall be responsible for the proper maintenance of all ICT equipment within the departmental premises, in order to ensure that all the equipment(s) are in best possible working conditions.

**13. Utilisation of ICT Assets and Resources**

*General*

- 13.1** Direct and indirect access to any Departmental website or webpage shall be subject to the website's terms and conditions;
- 13.2** Users must be authorised to obtain access to any system by a written allocation or authorisation, as the case may be, signed by the ICT Component/Unit and the Programme Manager of respective directorate as well as the system controller;
- 13.3** Any official who obtains access to any system without authorisation or without signing the User Declaration, or allows any other person(s) such access, shall be liable for any loss or damage incurred directly or indirectly as a result of such use of the system, whether or not the use in all other respects complied with the Departmental ICT Policy, and he/she must be charged with misconduct;
- 13.4** The authorised user is the custodian of any system allocated to him or her and as such owes a duty of care in respect thereof. Such system remains in his/her custody until such time as it is re-allocated to another official(s) or disposed off in writing;
- 13.5** In cases where circumstances dictate that a consultant(s) or any other official(s) from other state department(s) be given access to the Departmental ICT resources, permission may be granted by ICT Component/Unit on a needs basis provided that this is strictly for business;
- 13.6** All ICT Assets (hardware and software) shall:
- 13.6.1** Be strictly utilised by Departmental personnel for official purposes only as they are provided as working tools to enable them to perform their official functions diligently;

**13.6.2** Remain the property of the DCS&TM. Therefore, immediate family member(s), friend(s), relative(s) or non-officials of the department are NOT allowed to utilise Departmental ICT assets (hardware and software). This includes all mobile devices which officials often take home.

➤ ***Electronic Mail and internet***

**13.7** Internet services provided by Provincial IT, like other Government equipment and resources, are to be used only for authorized purposes, such as Government business, research, training, and professional development. Internet use requires responsible judgment, supervisory discretion, and compliance with applicable laws and policies;

**13.8** Internet and e-mail access remains a privilege not a right and the department still reserves the right to give access or refuse access without providing any reasons; Approval to access internet or e-mail shall be granted by the manager concern.

**13.9** Employees may not use the Department's internet services, including e-mail, for the following purposes during working or non-working hours:

**13.9.1** Engagement in matters directed towards the success or failure of a political party, Candidate for partisan political office, or partisan political group, or activity to support Political fund raising;

**13.9.2** Use that could generate or result in an additional charge or expense to the Government;

**13.9.3** Unauthorized creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented material/ Internet access to any other pornographic, abusive, and explicit site(s) and any other site(s) with reference to such site(s) on the departmental network;

**13.9.4** Participation in or encouragement of illegal activities or the intentional creation, downloading, viewing, storage, copying, or transmission of materials that are illegal or discriminatory;

**13.9.5** Use of Government e-mail addresses in a manner that shall give a false impression that an employee's otherwise personal communication is authorized or endorsed by the Department. An employee may not use his/her title, official designation or the Department when using Government e-mail for personal communications, because that might imply that the communication is official. If a personal e-mail or other electronic message could be misunderstood to be an official communication, the sender must clearly indicate that the message is of a personal nature. Engagement in any activity that would bring discredit on the Department or would violate any statute or regulation is prohibited.

➤ ***Legal and Illegal software***

**13.10** The loading of private software and storage of private data on department computers is prohibited;

**13.11** Any legally/illegally acquired software application program shall be removed or deleted, if no prior permission was granted by the ICT manager to acquire and utilise such software within the department;

- 13.12 Only trained ICT Component/Unit personnel or authorized personnel or vendor agent(s) is allowed to load any software on the department computers in consultation with the ICT Component/Unit;
- 13.13 Legal software is governed by the End-User License Agreement (EULA) between DCS&TM, the State Information Technology Agency (SITA) and the holder of proprietary rights. Therefore, all officials are expected to strictly adhere to the spirit and the letter of such an agreement at all times;
- 13.14 Loading of computer software games on department computers and utilizing department computers to play such games, is prohibited;

➤ **Storage of Personal Data & Information**

- 13.15 Storage of pornographic, abusive, explicit materials, data and any other information with reference to such site(s) on departmental computers, is strictly prohibited;
- 13.16 Storage of any of departmental information or data classified as TOP SECRET, RESTRICTED, CLASSIFIED and CONFIDENTIAL on all mobile computers is highly discouraged, due to the fact that mobile equipment are easily accessed by unauthorised persons or stolen during or after hours;
- 13.17 Servers shall strictly be used to store business related information or data, no personal or private information shall be stored on departmental servers;
- 13.18 Downloading of private software or any other software products from the internet by any other official in the department without the supervision of the trained ICT Component/Unit personnel or prior arrangement with the ICT Component/Unit is prohibited.

**14. ICT Support**

- 14.1 All calls for ICT services should be logged through the Provincial IT helpdesk. A reference number shall then be issued and the client must keep the reference number for later use if he/she wants to make a follow-up on an outstanding call(s);
- 14.2 If the call(s) remain unattended to for more than forty eight (48) hours and the client(s) did not receive any satisfactory explanation from any IT personnel, an outstanding call(s) must be referred in writing to the following officials in this order:
- **ICT Component/Unit Manager - for 48 hours**
  - **Chair of the ICT Steering Committee - for 72 hours**
  - **Head of Department - for 120 hours**
- 14.3 The client(s) should always have his/her reference number readily available when an enquiry of an outstanding call(s) is logged.

**15. Monitoring and Evaluation**

- 15.1 The implementation of the framework shall be monitored through financial cycle semester reports.



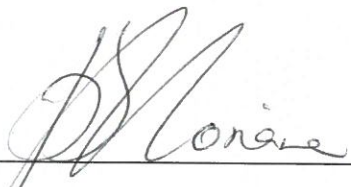
15.2 The ICT Steering / Strategic Committee shall evaluate the effectiveness of this framework through an annual review.

**16. Review of the Framework**

This framework shall be reviewed after 2 years upon the new developments that have been introduced within the Department.

**17. Approval**

This framework is agreed to by the Accounting Officer.



Handwritten signature of Mr. O. Mosiane in black ink, written over a horizontal line.

**MR O. MOSIANE  
ACTING HEAD OF THE DEPARTMENT**

21/07/16

**DATE**

