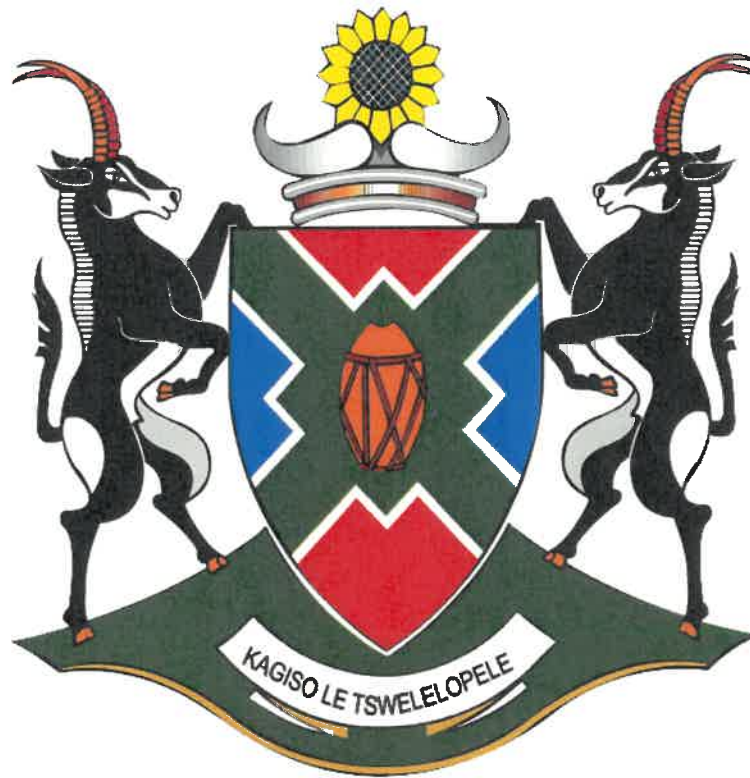


RESTRICTED

**DEPARTMENT OF COMMUNITY SAFETY & TRANSPORT MANAGEMENT**



**GOVERNANCE AND MANAGEMENT OF ICT FRAMEWORK**

**GMICTF—VERSION 1.4**


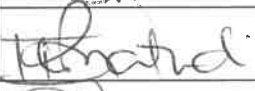


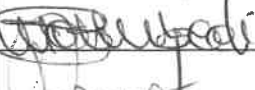

## Document Details

<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>	<Date of Accounting Officer's signature>
<b>Created Date</b>	30-06-2013
<b>Version Date</b>	<Date of Accounting Officer's signature>
<b>Version</b>	GMICTF-VERSION 1.4

## Change Record

Modified Date	Author	Version	Description of Changes
26-09-2014	Directorate Strategic Support Services	1.1	Departmental Business Change
21-07-2016	Directorate Strategic Support Services	1.2	Annual review
31-03-2018	Directorate Strategic Support Services	1.3	Annual Review
	Directorate Strategic Support Services	1.4	Review

## Stakeholder Sign-Off

Name	Position	Signature	Date
Mr S. Matlhako	Departmental Information Technology Officer		03/06/2021
Ms K. Phatudi	Governance Champion		28/05/2021
Ms F. Nchoe	Chairperson: ICT Steering Committee		01/06/2021
Ms M. Dayel	Chairperson: ICT Strategic Committee		03/06/2021
Ms M.G. Mothibedi	Departmental Chief Risk Officer		03/06/2021
Mr P. Namate	Director Legal Services		07/06/2021

## Records Management Sign-Off

Name	Position	Signature	Date
Ms M. Malatji	Deputy Director Records		11/06/2021

## Glossary of Terms

<b>Authorised user</b>	Any user who has been given credentials to access a departmental system
<b>CGICTPF</b>	Corporate Governance of ICT Policy Framework
<b>Corporate Governance</b>	<p><i>"...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."</i> (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>DITO</b>	Departmental Information Technology Officer
<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>EULA</b>	End-User License Agreement
<b>Governance</b>	The Senior Manager in the department who is responsible to drive Corporate Governance of and Governance of ICT.

<b>Champion</b>	
<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 strategy and objectives (ITGI 2005)</p> <p>The system by which the current and future use of IT is directed and Controlled.</p>
<b>Department / DCS&amp;TM</b>	The Department of Community Safety and Transport Management
<b>Accounting Officer</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>Lessor</b>	The owner of the property when rented by lease
<b>Lessee</b>	Department of Community Safety & Transport Management
<b>Medium Laptops</b>	17" or bigger
<b>MISS</b>	Minimum Information Security Standards
<b>MIOS</b>	Minimum Interoperability Standards
<b>Small Laptops</b>	15" or smaller

## TABLE OF CONTENTS

1. Introduction.....	1
2. Regulatory and Guidance Framework .....	1
3. Scope and Application.....	1
4. Purpose .....	2
5. Governance and Management .....	2
6. ICT Strategy.....	3
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.....	12
15. Monitoring and Evaluation.....	13
16. Review of the Framework .....	13
17. Approval.....	13

## **1. Introduction**

The Department recognises the significant advantages of using technology to enable efficiency of business processes and acceleration of service delivery. There are standing issues relating to ICT systems within the department as reflected in the successive Auditor General Reports. This policy document, therefore seeks to streamline Governance and Management of departmental ICT environment.

The Governance and Management of ICT policy is a subset of Corporate Governance of ICT and its proper implementation will ensure benefit realisation on investment in ICT.

## **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 Regulations
- Promotion of Access To Information Act

## **3. Scope and Application**

The framework is applicable to all employees within the Department 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 installed and configured ICT resources;
- 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 and the strategic alignment of ICT to the core business of the department in line with the approved departmental ICT Charter.

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

This committee shall coordinate and oversee the planning, implementation and execution of the Corporate Governance of ICT, strategic alignment of ICT to the business of the department, and shall 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 quarterly basis to the ICT Steering Committee on the implementation of the ICT implementation plan.

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

Governance Champion shall drive the implementation, change management and maintenance of Corporate Governance of ICT in the Department.

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

The DITO shall Align and execute ICT service delivery with the strategic goals and management plans of the Department.

**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 goals and management plans 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** Changes to the ICT Strategic Plan shall be effected as and when business or Technology changes present 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 Accounting Officer prior to **31 March 2021**.

## **7. ICT Management**

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



## **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 Department Information Technology Officer; and

8.1.3 Relevant ICT Governance 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;

8.2.2 Tested prior to implementation.

8.3 A Change Management plan that addresses the human behavioural and cultural aspects of the envisaged change shall be developed. A structured and pro-active communication and training programme shall be followed to ensure acceptance and buy-in from the departmental staff.

8.4 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.

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

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

8.7 All ICT projects should be processed through ICT Governance Structures.

8.8 ICT will not participate in projects that were processed outside ICT Governance Structures

## **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 relevant System Administrator;
- 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 and appropriate cooling levels. Where other risks may exist, these should be documented and appropriate counter-measures implemented.
- 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 computing 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;
- 9.6.3.1** Consistent and automated use of passwords across multiple systems insofar as the systems supports this.
- 9.6.3.2** Password protection at BIOS level; and
- 9.6.3.3** Automatic encryption of data.

**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 DITO.

**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** 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, DITO. The duly completion of such a handing-over certificate shall transfer custodianship to the new authorised user or Strategic Support Services, as the case may be.

## **11. ICT Contingencies**

- 11.1** The DITO shall ensure connectivity of the departmental users/systems to the network within the limits of their competency;
- 11.2** The DITO shall ensure that all System Administrators backup data on their respective servers in accordance with acceptable back up standards;

- 11.3** The DITO shall prepare an ICT Continuity Plan that includes a Disaster Recovery Plan, which is tested at least once a year; The execution of the ICT Continuity Plan and Disaster Recovery Plan is dependent on the Departmental Business Continuity Plan;
- 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 to the Chairperson of the Departmental Loss Control Committee through the Asset Management Unit / Security Management Unit. The official should compile a report that contains a copy of the statement and case number to the Chairperson of the Departmental Loss Control Committee through the Asset Management Unit / Security Management Unit to institute a formal investigation thereof.
- 11.5** If the outcome of the investigation reveals that the stolen/lost item(s) was due to the official's negligence, then the official(s) shall be held responsible for the loss suffered by the state. All officials are responsible for the safekeeping of all ICT resources allocated to them. Any direct or indirect damage to the 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;

## **12. ICT Procurement Framework**

### *General*

- 12.1** The requests for computing resources by Departmental users shall be directed to Supply Chain Management
- 12.2** In cases of requests for replacement of damaged/obsolete ICT resources, the Users shall log a call at IT Helpdesk on 018 388 1110 and the ICT Technician shall assess the computing resource and issue the ICT Technical Inspection report.
- 12.3** Supply Chain Management will advice users on what method/forms to use when requesting computing resources.
- 12.4** Strategic Support Services shall provide specifications for requested resources to Supply Chain Management (Quarterly)
- 12.5** Strategic Support Services shall load the necessary office productivity software onto the procured computing resources.

**12.6** Strategic Support Services shall provide the necessary network connectivity to the procured resources, and Administer Sign-offs of users (Allocation forms and declaration that the equipment received was in good working condition)

**12.7** Procurement of ICT resources and its allocation thereof shall be guided by the Supply Chain Management Processes and SITA contracts.

**12.8** *Mobile computing equipment*

The guidelines for distribution and use of computing equipment are:

➤ **Reasons for allocation of computing equipments**

- 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 employees or fixed term contract employees of the department are eligible for consideration of ICT resources. The finalization of the acquisition process shall be the responsibility of the Sub-Program Manager Supply Chain Management.

➤ **Cabling and Related Costs**

**12.9** Provincial IT is the custodian of Network Infrastructure, as such all requests relating to cabling shall be made to Provincial IT through DITO.

**12.10** The department is expected to submit network cabling needs for inclusion in the Provincial IT budget estimates for the following financial year.

**12.11** Lease Agreements which are managed by SCM should include inputs from ICT.

**12.12** The Department shall include network infrastructure design and installation in the planning and execution of current and future Departmental infrastructure projects

➤ ***Maintenance and Repairs***

**12.13** The ICT Component/Unit shall be responsible for the proper maintenance of all ICT equipments within the department, 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** Access to the recording for virtual meetings shall be made available to the Secretariat and the Chairperson of the meeting.

**13.3** Any other participants who need access to the meeting recording shall request approval from the Accounting Officer or Delegated Official.

**13.4** 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 Program Manager of respective directorate as well as the system controller;

**13.5** 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;

**13.6** 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;

**13.7** ICT resources are allocated to an individual as per his/her function; when the official is leave the office/ transferred/deployed the ICT resource shall be returned to the

Strategic Support Services directorate. The Sub/Program Manager/District Manager must ensure that the equipment is returned.

**13.8** 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 the Accounting Officer on a needs basis provided that this is strictly for business;

**13.9** All ICT Assets (hardware and software) shall:

**13.9.1** 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;

**13.9.2** Remain the property of the DCSTM. 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 and the information contained in the meeting recording is for official purpose only.

➤ ***Electronic Mail and internet***

**13.10** 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;

**13.11** Internet and e-mail access remains a privilege not a right and the department still reserves the right to give or deny access with valid reasons;

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

**13.12.1** 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;

- 13.12.2** Use that could generate or result in an additional charge or expense to the Government;
- 13.12.3** 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;
- 13.12.4** Participation in or encouragement of illegal activities or the intentional creation, downloading, viewing, storage, copying, or transmission of materials that are illegal or discriminatory;
- 13.12.5** Use of Government e-mail in a manner that shall give a false impression that an employee's other 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.
- 13.12.6** Engagement in any activity that would bring the Department into disrepute is prohibited.

➤ ***Legal and Illegal software***

- 13.13** The loading of private software e.g. games e.t.c. and storage of private data on department computers is prohibited;
- 13.14** Any legally/illegally acquired software application program shall be removed or deleted, if no prior permission was granted by the DITO to acquire and utilise such software within the department;
- 13.15** Only trained ICT Component/Unit personnel or authorized personnel or vendor agent(s) is allowed to load any authorised software on the department computers in consultation with the ICT Component/Unit;
- 13.16** Legal software is governed by the EULA between DCS&TM, the 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;



### ➤ ***Storage of Personal Data & Information***

- 13.17** Storage of pornographic, abusive, explicit materials, data and any other information with reference to such site(s) on departmental computers, is strictly prohibited;
- 13.18** 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;
- 13.19** Servers shall strictly be used to store business related information or data, no personal or private information shall be stored on departmental servers;
- 13.20** Downloading of any software products from the internet or any other source by any other official in the department without the supervision of the trained Departmental ICT personnel or prior arrangement with the Strategic Support Services 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 Departmental IT personnel, an outstanding call(s) must be referred in writing to the following officials in this order:
- **ICT Manager - for 48 hours of working days**
  - **Director Strategic Support Services - for 72 hours of working days**
  - **Chief Director Corporate Services - for 120 hours of working days**
- 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 a period of three (3) years or as and when there is a major change.

**17. RECOMMENDED/ ~~NOT RECOMMENDED~~**

All applicable prescripts/controls for  
compliance policies have been complied with  
without compromise



**MS B. MOFOKENG**  
**HEAD OF DEPARTMENT**

18/04/2021

**DATE**

**18. Approval**

This framework is agreed to by the Accounting Officer.



**MR M. MOKONYAMA**  
**ACCOUNTING OFFICER**

30/04/2021

**DATE**