DEPARTMENT OF COMMUNITY SAFETY AND TRANSPORT MANGEMENT

KAGISO LE TSWELELOPELE
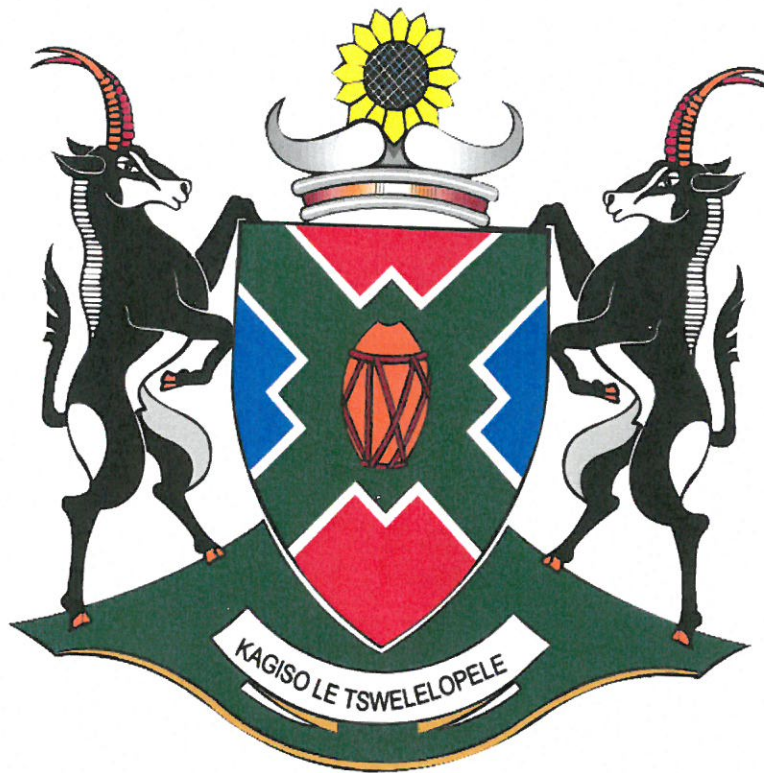
CORPORATE GOVERNANCE OF

INFORMATION COMMUNICATION AND TECHNOLOGY POLICY FRAMEWORK

(CGICTPF – VERSION 1.2)

Document Details

Author	Directorate Strategic Support Services
Department	Community Safety and Transport Management
Division Name	ICT Management
Document Name	Corporate Governace of ICT Policy Framework
Sensitivity	Internal Use Only
Effective Date	<After the HoD signature>
Created Date	01-04-2013
Version Date	<Date of HoD signature>
Version	CGICTPF-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

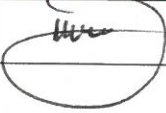| Name	Position	Signature	Date
Mr S. Matlhako	Departmental Information Technology Officer & Director Strategic Support		14/07/2016
Ms K. Phatudi	Strategic Committee Chairperson & Governance Champion		14/07/2016
Ms M.G. Mothibedi	Departmental Risk Management Officer		14/07/2016
Mr S. Setlhare	Acting Director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

Records Management Sign–Off

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

TABLE OF CONTENTS

Glossary of Terms

CGICTPF	Corporate Governance of Information Communication Technology Policy Framework
Corporate Governance	Procedures and processes according to which an organisation is directed and controlled. (Glossary of Statistical Terms – Organisation of Economic and Co-operation Development www.oecd.org)
Corporate Governance of Information Communication Technology (CGICT)	The system by which the current and future use of ICT is directed and controlled. 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)
DPSA	Department of Public Service and Administration
Executing Authority	Means the member of Provincial Executive Council responsible for Community Safety & Transport Management Portfolio
Executive Management	The Executive Management of the Department includes the Head of Department, Chief Directors , and Departmental Information Technology Officer (DITO).
GICT	Governance of Information Communication Technology
DITO	Departmental Information Technology Officer (Cabinet Memorandum 38(a) of 2000)
GITOC	Government Information Technology Officer's Council (Cabinet Memorandum 38(a) of 2000)
EA	Enterprise Architect
Governance Champion	The Executive Manager in the department who is responsible to drive Corporate Governance of and Governance of ICT.
Governance of ICT	The effective and efficient management of IT resources to facilitate the achievement of company strategic objectives. (King III Code: 2009: 52) 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) The system by which the current and future use of IT is directed and controlled.
Department	The Department of Community Safety and Transport Management
HoD	Head of Department

Dcs&tm	Department of Community Safety & Transport Management
ICT	Information and Communications Technology, also referred to as **IT**
ISO/IEC 38500	International Standard on Corporate Governance of ICT (ISO/IEC WD 38500: 2008: 1)
IT	Information Technology , also referred to as ICT
MISS	Minimum Information Security Standards
MIOS	Minimum Interoperability Standards

1. Introduction

The use of IT has become a fundamental business resource in organizations. No organization in the world today can function effectively without information technology and information systems. Information Technology has become such a critical resource for the success of any business or governmental organization.

Investments in information systems hardware, software, and telecommunications equipment now constitutes significant proportion of all capital investment in many organizations. The results of this massive spending in Information Systems and Technologies is reflected in the way organizations conduct business. Cell phones, messaging, wireless handhelds, e-mail, and online conferencing over the Internet have all become essential business tools.

Corporate Governance of ICT requires that all important ICT decisions should come from the senior political and managerial leadership and not delegated to ICT management. This accountability enables the department to align the delivery of ICT services with the department's strategic goals.

This policy framework provides for effective governance of ICT, to assist those at the highest level of the dcs&tm to understand and fulfil their legal, regulatory, and ethical obligations in respect of the department's use of Information Technology.

2. Regulatory and Guidance Framework

The following documents inform the development of this Policy framework for the department.

I. Public Service Act 103 of 1994

II. Public Service Regulations 2001

III. Public Finance Management Act 1 of 1999

IV. State IT Agency Act 88 of 1998

V. The Corporate Governance of ICT Framework

VI. CGICT Assessment Standard

VII. ISO/IEC 38500

VIII. Departmental Policies (SCM, Finance, HR, Risk, Security Security and Records Management)

IX. Office of the Premier ICT Policies

3. Scope of Application

This policy framework offers guiding principles for executive management of the department on the effective, efficient, and acceptable use of IT within the department. It applies to the governance of management processes and decisions relating to the IT services used by the department.

This policy applies throughout the department in as far as Corporate Governance of ICT is concerned.

4. Purpose

The purpose of this policy framework is to promote effective, efficient, and acceptable use of IT in the department by:

I. Embedding the Corporate Governance of ICT and Governance of ICT as a subset of Corporate Governance in the department.

II. Creating business value through ICT enablement by ensuring business and ICT strategic alignment.

III. Providing relevant ICT resources, organisational structure, capacity and capability to enable ICT service delivery.

IV. Achieving and monitoring ICT service delivery performance and conformance to relevant internal and external policies, frameworks, laws, regulations, standards and practices.

V. DITO should be appointed at executive level in order to represent the ICT function on Executive Management.

VI. Implementing the governance of ICT in the department, based on the DPSA framework.

5. Corporate Governance in the Department

5.1 The purpose of corporate governance is to create value for the department's stakeholders. It consists of a governance system that affects the way the department is managed and controlled. It also defines the relationships between stakeholders and the strategic goals of the department.

5.2 Corporate Governance structures in the department.

Oversight Reporting Structures

- Portfolio Committee
- EXCO
- EXTECH
- SCOPA

Internal Governance Structure

- MEC meetings
- DMC
- EDMC
- IT Governance Committees

5.3 Corporate governance is also concerned with individual accountability and responsibilities within a department. It describes how the department is directed and controlled and is in particular concerned with the following:

a) Organisation - the organisational structures, and coordinating mechanisms (such as steering forums) established within the institution and in partnership with external bodies;

b) Management - the individual roles and responsibilities established to manage business change and operational services; and

c) Policies - the frameworks established for making decisions and the context and constraints within which decisions are taken.

5.4 The executive leadership, which is accountable, provides the strategic direction of the department. The strategic direction, together with the external and internal context, determines the strategic goals. Corporate Governance of and the Governance of ICT are executed at Executive Management level through the function of evaluation, direction and monitoring. The management of business execution is done through the organisational structure and utilisation of the relevant resources.

5.5 The Executive Leadership and Management of the department are accountable and responsible For implementing a governance system.

6. Corporate Governance of ICT in the Department

6.1 The Corporate Governance of ICT is a subset of Corporate Governance and is an integral part of the governance system. In terms of such a system:

(a) the **Executing Authority** provides the political leadership;

(b) the **Head of Department** provides the strategic leadership and is accountable for the implementation of the Corporate Governance of ICT; and

(c) **Executive Management** is responsible for ensuring that the Corporate Governance of ICT is implemented and managed.

The department has established three ICT Committees which includes ICT Startegic Committee, ICT Steering Committee and ICT Operational Committee. These committees derive their mandate from the departmental ICT Charter.The roles and responsibilities of this committee structures are well defined in the ICT Charter of the department *(reference to Page 2 ICT Charter)*. Furthermore, the sittings of this committees are quarterly. The departmental ICT Plan shall ensure that ICT is aligned to the departmental Strategic Goals and Objectives.

6.2 The Corporate Governance of ICT involves evaluating and directing the achievement of strategic goals and using ICT to enable the departmental business and the monitoring of ICT service delivery to ensure continuous service improvement. It includes determining strategic goals, plans and Annual Performance Plans for ICT service delivery.

6.3 The HoD and Executive Management are respectively accountable and responsible for implementing the Corporate Governance of ICT in the department. Effective Corporate Governance of ICT is achieved in the department through:

(a) Institutionalising a Corporate Governance of ICT Policy Framework that is consistent with the Corporate Governance of the department;

(b) Aligning the ICT strategic goals with the departmental strategic goals;

(c) Ensuring that optimum business value is realised from ICT-related investment, services and assets;

(d) Ensuring that business and ICT-related risks do not exceed the departmental risk appetite and risk tolerance;

(e) Ensuring that ICT-related resource needs are met in an optimal manner by providing the organisational structure, capacity and capability;

(f) Ensuring that the communication with stakeholders is transparent, relevant and timely; and

(g) Ensuring transparency of performance and conformance and driving the achievement of strategic goals through monitoring and evaluation.

7. The Principles for the Corporate Governance of ICT

7.1 This Corporate Governance of ICT Policy Framework in the department is based on the seven principles adopted by the DPSA in the CGICTPF, as explained in the international good practice and standards for ICT governance, namely, King III Code, ISO/IEC 38500. The adopted principles are:

(a) *Principle 1: Political Mandate*-The Executive Authority must ensure that Corporate Governance of ICT achieves the political mandate of the department.

(b) *Principle 2: Strategic Mandate* - The HoD must ensure that Corporate Governance of ICT achieves the department's strategic plans.

(c) *Principle 3: Corporate Governance of ICT* - The HoD must create an enabling environment in respect of the Corporate Governance of ICT within the applicable legislative and regulatory landscape and information security context.

(d) *Principle 4: ICT Strategic Alignment* - Executive Management must ensure that ICT service delivery is aligned with the departmental strategic goals and that business accounts for current and future capabilities of ICT. It must ensure that ICT is fit for purpose at the correct service levels and quality for both current and future business needs.

(e) *Principle 5: Significant ICT Expenditure* - Executive Management must monitor and evaluate major ICT expenditure, ensure that ICT expenditure is made for valid business enabling reasons, monitor and manage the benefits, opportunities, costs and risks resulting from this expenditure, while ensuring that information assets are adequately managed.

(f) *Principle 6: Risk Management and Assurance - Executive* Management must ensure that ICT risks are managed within the departmental risk management practice. It must also ensure that the ICT function is audited as part of the departmental audit plan.

(g) *Principle 7: Organisational Behaviour* - Executive Management must ensure that the use of ICT demonstrates the understanding of and respect for organisational behaviour/culture.

8. The Corporate Governance of ICT Practices

The Corporate Governance of ICT practices shall be used to cascade the principles for implementation in the department. In which,

8.1 The Executing Authority shall:

(a) provide political leadership and strategic direction, determine policy and provide oversight;

(b) ensure that ICT service delivery enables the attainment of the strategic plan;

(c) take an interest in the Corporate Governance of ICT to the extent necessary to ensure that a properly established and functioning Corporate Governance of ICT system is in place in the department to leverage ICT as a business enabler;

(d) assist the HoD to deal with intergovernmental, political and other ICT-related business issues beyond their direct control and influence; and

(e) ensure that the department's organisational structure makes provision for the Corporate Governance of ICT.

8.2 The Head of Department shall:

(a) provide strategic leadership and management;

(b) ensure alignment of the ICT strategic plan with the departmental and business strategic plans;

(c) ensure that the Corporate Governance of ICT is placed on the department's strategic agenda;

(d) ensure that the Corporate Governance of ICT Policy Framework, charter and related policies for the institutionalisation of the Corporate Governance of ICT are developed and implemented by Executive Management;

(e) determine the delegation of authority, personal responsibility and accountability to the Executive Management with regards to the Corporate Governance of ICT;

(f) ensure the realisation of department-wide value through ICT service delivery and management of business and ICT-related risks;

(g) ensure that appropriate Corporate Governance of and Governance of ICT capability and capacity are provided and a suitably qualified and experienced Governance Champion is designated, who must function at Executive Management level;

(h) Ensure that appropriate ICT capacity and capability are provided and a suitably qualified and experienced DITO, who must function at Executive Management level, is appointed; and

(i) Ensure the monitoring and evaluation of the effectiveness of the Corporate Governance of ICT system.

8.3 Risk and Audit Committee shall:

Assist the HoD in carrying out his/her Corporate Governance of ICT accountabilities and responsibilities.

8.4 Executive Management shall ensure:

(a) ICT strategic goals are aligned with the department's business strategic goals and support strategic business processes; and

(b) Business-related ICT strategic goals are cascaded throughout the department for implementation and are reported on.

(c) Means and Mechanisms:

    i. Advice is provided to the HoD regarding all aspects of the Corporate Governance of and Governance of ICT;

    ii. The Corporate Governance of and Governance of ICT is implemented and managed;

    iii. The necessary strategies, architectures, plans, frameworks, policies, structures (including outsourcing), procedures, processes, mechanisms and controls, and culture regarding all aspects of ICT use (business and ICT) are clearly defined, implemented, enforced and assured through independent audits;

    iv. The responsibility for the implementation of the Corporate Governance of and Governance of ICT is delegated and communicated to the relevant management (senior business and ICT management);

    v. Everyone in the department understands the link between business and ICT strategic goals and accepts their responsibilities with respect to the supply and demand for ICT;

    vi. The planning and execution of ICT adheres to relevant judicial requirements; and

    vii. ICT-related risks are managed.

(d) ICT Security:

    i. An information security strategy is approved;

    ii. Intellectual property in information systems is appropriatelyprotected; and

    iii. ICT assets, privacy, security and the personal information ofemployees are effectively managed.

(e) Organisational Behaviour/Culture:

    - The use of ICT demonstrates the understanding of and respect for organisational behaviour/culture, which should include humanbehaviour.

(f) All services rendered by third parties shall be managed through SLA and/or contracts.

9   CGICT Roles and Structures

9.1 Within the governance system, the CGICT and GICT are executed on Political and Strategic Leadership, Executive Management, Business and Operational levels. Different decision making forums should be established to support the Political and Strategic Leadership and Executive Management in the performance of their CGICT duties.

9.2 The Accounting Officer shall appoint an ICT Governance Champion, an Executive Manager in the department, who shall be responsible to drive Corporate Governance of and Governance of ICT.

9.3 The Governance Champion shall:

(a) be atleast a senior manager at least on the level of a Chief Director who reports to Executive Management. He/she must be an authoritative and articulate person with strong decision-making abilities and the mandate to make decisions and escalate deviances and problems;

(b) have a clear understanding of the department's core functions;

(c) be actively involved in the oversight of the formal Corporate Governance System of the department;

(d) facilitate the alignment process between business and ICT strategy and plans;

(e) be responsible for developing, implementing, maintaining and communicating the necessary Corporate Governance of ICT policies, structures, processes, procedures, mechanisms, controls/(effective and useful measures), charter and plan;

(f) oversee that the Governance of ICT system, as a subset of Corporate Governance of ICT is developed, implemented and maintained; and

(g) be supported by a cross-functional team, which must include representatives from business and the DITO.

9.4 The Accounting Officer shall establish the following committees set out below to assist the political and strategic leadership and the ICT Governance Champion in carrying out their duties with regard the corporate governance of ICT and the Governance of ICT:

9.4.1 *ICT Strategic Committee* –

(a) which 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;

(b) Munites/ resolutions/recommendations approved by the chairperson of the committee and attendance register of this committee shall be forwarded to the Accounting Officers after every quarterly sitting and recommendations approved by the Accounting Officer might have to be announced at Departmental Management Committee (DMC) if deemed necessary by the Accounting Officer.

(c) Shall ensure progress on all ICT Audits through departmental Audit Steering Committee to advocate for good governance.

9.4.2 *ICT Steering Committee* –

(a) which 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; and

(b) This committee shall report its deliberations of every quarterly sitting to the strategic committee.

(c) Shall ensure that ICT related risks are monitored for quality and implementation.

9.4.3 *ICT Operational Committee –*

(a) which 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;

(b) This committee shall report its findings to the Steering committee.

(c) Shall assist in trying to curb the challenges with regard to loss of ICT resources.

9.5 The *DITO* function was established in the department to align and execute ICT service delivery with the strategic goals and management plans of the department. The DITO function shall ideally be positioned at an Executive Management level, such that the function can be represented at the strategic management level in the department. The DITO is the most senior official of the department who is responsible for aligning ICT and business strategies and shall be responsible for planning, resourcing and managing the delivery of ICT services and solutions to support departmental strategic objectives. The DITO shall therefore be responsible for the following key practices:

- Alignment of ICT to business strategy;

- Manage Business and ICT relationship;

- Operationalise ICT strategic plan through implementation; and

- Identify opportunities, risk and constraints for ICT to enhance the department.

9.5.1 The department is represented at the Provincial GITO Council by the DITO.

10 ICT Stakeholders in the Department

10.1 The following table outlines the key internal and external stakeholders with their roles and functions that have a direct influence on the Corporate Governance of ICT policy in the department:

List of Stakeholders	Roles and Functions
Executive Authority	Provide political leadership for the department
Head of Department	Provide strategic leadership in the department
Executive Management	- Provide a support function to the various structures and strive towards appropriate execution and implementation of ICT Governance operations within the department - Ensure that ICT goals are aligned to the business and ICT Strategy of the organisation - Ensure conformance and performance measures and reporting of ICT and ICT Governance Ensure that business owners shall oversee ICT Service delivery in support of their business

	enablement
Auditor General South Africa (AGSA)	Auditing functions on good governance and compliance to legislation.
Provincial Internal Audit – ICT Auditor	provide an appropriate oversight and advisory role to the department to improve on ICT Governance.
Enterprise Architect (EA Office of the Premier)	A person knowledgeable in the business of the department or at provincial IT, who shall be responsible for the structured planning to articulate the business and related processes of the department in an interrelated and standardised way
Chief Risk Officer	Implements the Departmental Risk Management Strategy that includes ICT Risks
Chief Financial Officer	Provides financial management and support
Provincial GITO Council	- Provincial Government Information Technology Officer provides strategic direction on ICT issues. - Provides shared ICT Services and connectivity infrastructure for all provincial departments.
ICT Manager	responsible for the operational management of ICT
Business Owners	End users of ICT services
Security Services	Minimum Information Security Standards unit responsible for overall security of the department.
Departmental Management Commitee (DMC)	This committee be timeously notified prior the event, for any possible change as a result of ICT developments that might affect departmetal business.
Provincial IT (Office of the Premier)	Office at which IT network infrastructure in the province is centralised.

11   Business and ICT alignment Planning

11.1 The ICT Strategic Committee shall be responsible for the development of a departmental ICT Strategic Plan that is aligned to the business processes, requirements and the five year strategic plan of the department.

11.2 The ICT Strategic Plan should cover at least the Medium Term Expenditure Framework (MTEF) or the Medium Term Strategic Framework (MTSF), which spans the 5 year electoral cycle.

11.3 The ICT Strategic Plan must be updated at least annually but more frequently should business or technology changes present risks or opportunities that should be reflected in the plan.

11.4   The ICT Strategic Plan must contain at least:

(a) A clear definition of the current business processes and requirements of the Department;

(b) Statements of expected changes in the business and structure of the Department over the coming three years;

(c) Descriptions of the capabilities of the existing ICT infrastructure;

(d) Evaluation of the gaps between the current and future business ICT requirements of the Department and the capabilities of the existing ICT infrastructure;

(e) Proposals to eliminate the gaps referred to in (d) above; and

(f) Documentation of new technologies, their likely impact on the business of theDepartment and their expected cost.

12 Prescriptive landscape

12.1 Public Service Regulations

The Public service regulations inform CGICT in several areas:

(a) Delegations of Authority in terms of Part II principles:

  i. The HoD must delegate responsibilities for ICT;

  ii. Employees must be empowered to make decisions.

(b) Strategic Planning and ICT Alignment:

  i. There must be an Information Systems to monitor progress;

  ii. ICT should provide information for strategic planning;

  iii. ICT should support compliance requirements of the department.

(c) Information Planning and Reporting require the HoD to develop:

  i. An Information Plan aligned to the Strategy;

  ii. An Infrastructure Plan to support the Information Plan;

  iii. An Operational Plan for Information and ICT Infrastructure Management.

(d) e-Government Regulations:

  i. ICT acquisition shall be based on making the department effective, efficient, and improve service delivery directly or indirectly;

  ii. Information Security need requires a different breed of security for e-Government and compliance to Minimum Information Security Standard (MISS) is required;

  iii. Compliance to Interoperability Standards as with defined in the Minimum Interoperability Standard (MIOS) for each ICT project.

12.2 Public Finance Management Act

(a) The PFMA is applicable to ICT in the financial planning and acquisition of ICT resources and risk management. Procurement and management of ICT assets shall be executed in accordance with the PFMA.

12.3 SITA Act

The State Information Technology Agency provides ICT services to government. The SITA act requires that all ICT goods and services shall be sourced through SITA to achieve economies of scale and standardisation. The department shall align its acquisition processes to SITA as required by the SITA act.

12.4 ICT Related Policies

All ICT functions, plans and operations shall be guided by the following approved documents:
- Corporate Governance of ICT Policy Framework (CGICTPF)
- Governance and Management of ICT Framework (GMICTF).
- ICT Charter (CGICTC).
- ICT Security Policy (ICTSP)
- ICT Portfolio Management Framework (ICTPMF)
- ICT Continuity Plan (ICTCP)
- Deaprtmental Enterprise Risk Management Policy
- Supply Chain Management Policy Guide on Procurement and Asset Management (IT related furniture and equipment) and Processes.
- Finance Management Policies e.g. Asset Loss Contro e.t.c.
- Human Resources Management Policies i.e. Training and Developments, Leave management e.t.c, and
- Observe any other policies deemed relevant/necessary to ICT by the department.

All departmental business systems (including those hosted at Office of the Premier) shall be governed by the following policies either developed departmentaly or at Provincial Level (Office of the Premier):
- User Account Management Policy and/or procedures;
- Information Security Policy;

However in the event were both institutions (i.e. the department and Office of the Premier) have both developed the same above mentioned policies, the departmental developed policy shall take precedence especially for department specific systems, an exemption however shall be given to transversal systems.

The operational environment at which departmental systems are hosted at provincial or departmental level shall be compliant to the minimum environmental set standards i.e acceptable room temperature (Cool) and/or with enough ventilation, for both facilities, patch rooms and servers. However the approved standard by Office of the Premiere shall be made available to the department.

The department shall ensure the existence of configuration standards or technical Procedure Manual which include every business system in the department.

13 Enabling Policies and Plans

The following are minimum enabling policies in the department:

13.1 Enterprise Architecture Plan

The Strategic Enterprise Architecture (EA) services which is centralised at Provincial IT shall facilitate the development of the departmental EA Plan. The plan will be based on the Government Wide Enterprise Architecture (GWEA) framework and shall be developed in the third iterative phase as continious improvement. However, the plan shall be linked to the ICT expenditure.

13.2 Enterprise Risk Management Policy

The departmental Enterprise Risk Management policy shall be used to continually identify, assess and reduce ICT-related risks within levels of tolerance set by Executive Management. ICT Risk Management in the department shall be guided by the approved Departmental Enterprise Risk Management Policy through the recent ICT Risk Register.

13.3 Internal Audit Standards

The department shall utilise the internal audit standards which are developed/guided by the Provicial Internal Audit (PIA) and/or Auditor General(AG) to ensure good governance and compliance to legislation..

13.4 ICT Portfolio Management Framework

ICT related projects in the department shall be guided by the approved project portfolio management which include methodologies for managing its ICT projects. The ICT Portfolio Management Framework shall be defined to ensures consistent, efficient,and effective implementation of the portfolio of projects as undertaken by the ICT Directorate.

13.5 ICT Security Policy

The Accounting Officer shall ensure that classified information, intellectual property and personnel information are protected within ICT systems. The ICT Security Policy informs the ICT Security Plan.

13.6 Business Continuity Plan (BCP)

The Department shall develop a Business Continuity Policy and Plan that enables critical departmental services to be continually delivered to clients even after disaster has striken.The developed Business Continuity Plan shall inform ICT Continuity Plan.

14 Change Management Plan

The department shall have a Change Management Policy and Change Management plan that addresses the human behavioural and cultural aspects of the change. A structured and pro-active approach should be followed to ensure acceptance and buy-infrom Political and Strategic Leadership to operational staff of the department.

15 Review of the Policy

This policy shall be reviewed annually depending upon the new developments that have been introduced within the Department.

16 Monitoring and Evaluation

The implementation of the policy shall be monitored through semester reports. The ICT Strategic Committee shall evaluate the effectiveness of this policy through annual policy review.

17 Approval

This policy shall come into operation from the effective date i.e. the date upon which it has been signed off and approved by the Accounting Officer.

MR O. MOSIANE
ACTING HEAD OF THE DEPARTMENT

21/07/16

DATE