Information and Communication Technology Management Framework

<table>
<thead>
<tr>
<th>APPROVED/REVIEWED</th>
<th>COUNCIL MEETING DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 2017 / March 2020</td>
<td>29 March 2017</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

1. PREAMBLE .................................................................................................................. 3
2. LEGAL FRAMEWORK .................................................................................................. 3
3. DEFINITIONS ............................................................................................................... 4
4. SCOPE .......................................................................................................................... 5
5. INTRODUCTION ........................................................................................................... 5
6. ICT MANAGEMENT PRINCIPLES .............................................................................. 7
7. IMPLEMENTATION OF THE FRAMEWORK: ........................................................... 7
   7.1 ACCESS MANAGEMENT ......................................................................................... 7
   7.1.1 ACCESS MANAGEMENT POLICY ..................................................................... 7
   7.2 ICT SERVICE PROVISION, MANAGEMENT AND CONTROL .................................. 7
      7.2.1 CHANGE MANAGEMENT POLICY ................................................................. 7
      7.2.2 INCIDENT MANAGEMENT POLICY ............................................................... 7
      7.2.3 RISK MANAGEMENT PRACTICE ..................................................................... 8
      7.2.4 SERVICE PROVIDER MANAGEMENT FRAMEWORK .................................... 8
      7.2.5 BUSINESS AND ICT SERVICE LEVEL AGREEMENT MANAGEMENT .... 8
      7.2.6 INFORMATION TECHNOLOGY TECHNICAL FRAMEWORK ....................... 8
   7.3 IMPLEMENTATION MANAGEMENT ......................................................................... 8
      7.3.1 SYSTEM DEVELOPMENT LIFE CYCLE METHODOLOGY .............................. 8
      7.3.2 PROJECT MANAGEMENT METHODOLOGY ............................................... 8
   7.4 SAFE GUARDING .................................................................................................... 8
      7.4.1 ICT CONTINUITY POLICY .......................................................................... 8
      7.4.2 ICT BACKUP AND RECOVERY MANAGEMENT POLICY .......................... 9
   7.5 NETWORK MONITORING PRACTICE .................................................................... 9
8. AWARENESS TRAINING ............................................................................................... 9
9. COMPLIANCE ............................................................................................................... 9
10. ADMINISTRATION OF THIS POLICY ....................................................................... 9
1. PREAMBLE

Information and communication technologies (ICT) are increasingly used as a strategic enabler of the business of the municipality. Through the strategic leadership of the Council and executive there is a continuous closer alignment between the municipal business and the use of ICT in its delivery. In this regard, service delivery, in all its aspects contain information in any of its life cycle phases: creation, transport, storage, retention and retirement. Information is carried in processes and processes are enabled through the use of ICT. This positions the municipality to use ICT in the realisation of value in all aspects of its business whether it be supporting operations or management, service delivery or serving the citizenry more effectively. In this, ICT facilitates interaction between people, process and the delivery of management practice. ICT then also inevitably finds its way into enabling monitoring and evaluation. There is thus nearly no area of the municipal business that ICT will not influence.

It is thus important that the same vigilance be applied to the use of ICT in service delivery as with normal business practice. The following risk areas are addressed in this Information and Communication Technology Framework (herein called the Framework):

- Curb a fragmented and uncoordinated approach to the use of ICT in service delivery leading to unmanageable diversity which can lead to fruitless and wasteful expenditure;
- All possible ICT measures be put in place to mitigate the risk of compromised ICT enabled business processes and information;
- Curb illegal access to and the misuse of and exploitation of information; and
- Protect citizens and employees against on-line identity theft.

The implementation of this Framework will provide reasonable means and practice to ensure that the municipal electronic information and processes are protected and managed, through ICT, from a technology perspective.

2. LEGAL FRAMEWORK

The policy was drafted bearing in mind the legislative conditions, as well as to leverage internationally recognised ICT standards.

The following legislation, among others, were considered in the drafting of this policy:

- Copyright Act, Act No. 98 of 1978
- Electronic Communications and Transactions Act, Act No. 25 of 2002
- Minimum Information Security Standards, as approved by Cabinet in 1996
- Municipal Finance Management Act, Act No. 56 of 2003
- Municipal Structures Act, Act No. 117 of 1998
- Municipal Systems Act, Act No. 32, of 2000
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996
- National Archives Regulations and Guidance
- Promotion of Access to Information Act, Act No. 2 of 2000
- Protection of Personal Information Act, Act No. 4 of 2013
- Regulation of Interception of Communications Act, Act No. 70 of 2002
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following internationally recognised ICT frameworks and standards were leveraged in the development of this policy:

- Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014
- Control Objectives for Information Technology (COBIT) 5, 2012
- King Code of Governance Principles, 2009

### 3. DEFINITIONS

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Management</td>
<td>To enable access to electronically stored information through the use ICT for approved municipal employees in a structured and controlled manner whilst maintaining electronic information safety and ensuring segregation of duties.</td>
</tr>
<tr>
<td>Alignment</td>
<td>The process of planning for and using ICT as an enabler of business service delivery to improve reliability, integrity and availability.</td>
</tr>
<tr>
<td>Business enablement</td>
<td>The use of ICT to enable in service delivery.</td>
</tr>
<tr>
<td>Change Management</td>
<td>Change Management refers to structured and authorised approach to transitioning the use of ICT in service delivery form an as-is to a to-be state.</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>Terminology</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ICT Continuity Management</td>
<td>The creation of plans through which ICT reduces vulnerability to hazards and cope with interruptions of its service to the business. It does not avert or eliminate the threats; instead, it focuses on creating plans to decrease the effect of interruptions.</td>
</tr>
<tr>
<td>Incident Management</td>
<td>Activities of the Senior Manager ICT to identify, analyse, and correct hazards to prevent a future re-occurrence.</td>
</tr>
<tr>
<td>Electronic Information</td>
<td>Information created by, transported through, stored in and managed utilising information systems.</td>
</tr>
<tr>
<td>Information System</td>
<td>An information system is computerised system for the collection, organization, storage and communication of information used to collect, filter, process, create and distribute electronic information.</td>
</tr>
<tr>
<td>Network</td>
<td>The computer infrastructure of the municipality that allows computers to interact internally and with the Internet and all the types of traffic that are facilitated by it.</td>
</tr>
<tr>
<td>Public Sector Risk Management</td>
<td>A publication by National Treasury on Risk Management Practice in the Public Sector in 2010.</td>
</tr>
<tr>
<td>Realisation of value</td>
<td>The use of ICT to assist the business in creation of value for operations, management, monitoring and service to the citizenry.</td>
</tr>
<tr>
<td>Technology</td>
<td>See ICT</td>
</tr>
</tbody>
</table>

4. SCOPE

This Framework applies to all staff and line function units, ICT related service providers, ICT department and users of electronic information resources within the municipality.

5. INTRODUCTION

The Municipal Corporate Governance of Information and Communication Technology (ICT) Policy (herein called the Policy) was approved by the Council on 29 September 2015. The Policy adopts a dual approach to the implementation of the Corporate Governance of ICT (CGICT). Firstly, the implementation of means and mechanisms to govern the use of ICT in service delivery at an executive level. This involves the actions of evaluating the municipal business landscape and the value that the use of ICT can create, directing how ICT will be used in enabling service delivery and monitor whether the value was created.
Secondly, it involves structuring of the ICT Department through means and mechanisms to efficiently and effectively manage the operational environment of ICT in support of the business requirements. This involves definition of this ICT Management Framework (herein called the Framework).

This Framework is implemented according to the model in Diagram 1. This model depicts the following:

5.1 **Access Management** – The conditions and management practices for providing user access to applications, information systems and back-end enabling systems. It furthermore addresses the baseline technology configuration and settings required to ensure reasonable security of data and electronically stored information.

5.2 **ICT Service Provisioning, Management and Control** – The controlled environment within which the ICT Department operates and manages the ICT enablement of service delivery. This includes areas such as information system and application provisioning, change, incident, technology infrastructure, service level and risk management.

5.3 **Implementation Management** – The structured management of projects.

5.4 **Safe Guarding** – The provision of ICT continuity planning, technology infrastructure and management and backup and restore service.

![Diagram 1. ICT Management Model](image)

The Framework thus provides the environment for efficient and effective management of ICT in service delivery. The implementation of this Framework is informed by principles presented in the following paragraph.
6. ICT MANAGEMENT PRINCIPLES

**Principle 1. Access Management**

The Municipal Manager must ensure that access to applications, information systems and back-end information technology be granted to approved natural persons in line with the business requirements of the municipality and are managed accordingly.

**Principle 2. ICT Service Provision, Management and Control**

The Municipal Manager must ensure that the use of and provisioning of ICT in service delivery is provided efficiently and effectively in a secured environment.

**Principle 3. Implementation Management**

The Municipal Manager must ensure that the implementation of, and changes to existing technology infrastructure, applications, information systems are planned and coordinated according to a structured approach under the leadership of the business owner.

**Principle 4. Safe Guarding**

The Municipal Manager must ensure that the life cycle continuity of electronically stored information and data is protected according to the business requirements.

7. IMPLEMENTATION OF THE FRAMEWORK:

This Framework is implemented via the following practices, policies and frameworks.

7.1 ACCESS MANAGEMENT

7.1.1 ACCESS MANAGEMENT POLICY

Information systems owners in cooperation with the Senior Manager ICT must ensure that access to ICT assets, electronically stored information and technology is authorised and restricted based on the municipal business requirements and segregation of duties. (See Access Management Policy)

7.2 ICT SERVICE PROVISION, MANAGEMENT AND CONTROL

7.2.1 CHANGE MANAGEMENT POLICY

The Senior Manager ICT in cooperation with information systems owners must ensure that changes to technology resources, applications and information systems may only be performed in a structured and controlled manner to ensure that changes do not compromise the business integrity of the municipality. (See Change Management Policy)

7.2.2 INCIDENT MANAGEMENT POLICY

The necessary measures are implemented to limit the probability of the occurrence of incidents that have the likelihood of compromising ICT enabled business processes or
electronically stored information and data. (See Incident Management Policy to be developed in 2017/18)

7.2.3 **RISK MANAGEMENT PRACTICE**
ICT risks must be managed in line with the risk management practice of the municipality in accordance with the National Treasury Risk Management Framework (2010).

7.2.4 **SERVICE PROVIDER MANAGEMENT FRAMEWORK**
Services received from service providers shall be managed through a service level agreement by the business owner in order to ensure that the expected business value is realised from the engagement. (See Service Level Agreement Framework)

7.2.5 **BUSINESS AND ICT SERVICE LEVEL AGREEMENT MANAGEMENT**
The services rendered to the business of the municipality by ICT will be managed according to a Service Level Agreement. (See Generic Service Level Agreement)

7.2.6 **INFORMATION TECHNOLOGY TECHNICAL FRAMEWORK**
The technological architectural baseline and its related security, integrity, availability and reliability is provided according to a structured and managed environment. (See Information and Communication Technology Framework)

7.3 **IMPLEMENTATION MANAGEMENT**

7.3.1 **SYSTEM DEVELOPMENT LIFE CYCLE METHODOLOGY**
The process and methodology for the development of information systems shall be managed under the leadership of business owners within a defined system development life cycle practice. (See System Development Life Cycle Methodology – to be developed in 2016/17)

7.3.2 **PROJECT MANAGEMENT METHODOLOGY**
Business enabling ICT projects shall be managed under the leadership of the business owner within a defined project management practice. (See Project Management Methodology- to be developed in 2016/17)

7.4 **SAFE GUARDING**

7.4.1 **ICT CONTINUITY POLICY**
ICT continuity is a subset of the municipal business continuity management practice. This practice determines the municipal ICT related requirements in a Business Continuity Plan. This shall form the basis for the formulation of an ICT Continuity Policy
and Plan. An ICT Continuity Strategy, Policy and Plan must be created. (See ICT Continuity Policy)

7.4.2 ICT BACKUP AND RECOVERY MANAGEMENT POLICY
Data stored on the infrastructure of the municipality shall be backed up and restorable according to its individual business requirements. (See ICT Backup and Recovery Policy.)

7.5 NETWORK MONITORING PRACTICE
The Municipal Manager authorises the monitoring of municipal network and delegates it to the ICT Senior Manager. Users of the municipal network are made aware that the network traffic is being monitored. The user accepts this condition on the log-on screen. This is done to monitor the network for security purposes and to track the performance of the network, applications and information systems.

8. AWARENESS TRAINING
ICT and security awareness shall be communicated to the municipality through the Communication Department.

9. COMPLIANCE
Any failure to comply with this policy is deemed to be misconduct and will be dealt with accordingly.

10. ADMINISTRATION OF THIS POLICY
The Senior Manager ICT is responsible for the maintenance of this policy. This policy will be reviewed at least on a 3-yearly basis.