ICT POLICIES

AND

FRAMEWORK

TABLE OF CONTENT

ICT POLICIES

TABLE OF CONTENTS

Municipal Corporate Governance of Information and Communication Technology Policy

EXECUTIVE SUMMARY

Information Communication Technology (ICT) Governance has been described as the effective and efficient management of ICT resources and processes to facilitate the achievement of Municipal goals and objectives. The ICT Governance Institute describes ICT Governance as, "...the responsibility of the board of directors and executive management."
ICT Governance has risen in importance because of the widening gulf between what the organization expects and what ICT delivers. ICT has grown to be seen as a cost centre with growing benefits to the organisation ICT serves. An ICT Governance framework is meant to align ICT functions to the organizational goals, minimise the risk ICT introduces and ensure that there is value in the investment made in ICT.

The view that ICT should be governed and managed at all levels within a given organizational structure is supported by internationally accepted good practice and standards. These practices and standards are defined in the King III Code of Good Governance, ISO 38500 Standard for the Corporate Governance of ICT and other best practice ICT Process Frameworks which forms the basis of this document.

Translated into a municipal operating environment the corporate governance of ICT places a very specific responsibility on the Council and Management within a municipality to ensure that the decision making process for ICT related investments and the operational efficiencies of the municipalities ICT environments remain transparent and are upheld. This accountability enables the municipality to align the delivery of ICT services with the municipality's Integrated Development Plans and strategic goals.

The Council and Management of municipalities need to extend their governance functions to include the Corporate Governance of ICT. In the execution of the Corporate Governance of ICT, they should provide the necessary strategies, architectures, plans, frameworks, policies, structures, procedures, processes, mechanisms and controls, and culture which are in compliance with the best practise ICT Governance Frameworks.

To strengthen the Corporate Governance of ICT further, responsibility for the decision making of ICT programmes and projects should be placed at a strategic level in the municipality. The Corporate Governance of ICT is a continuous function that should be embedded in all operations of a municipality, from Council and Management level to all areas within a municipality including ICT service delivery.

According to the establish frameworks, the Governance of ICT is implemented in two different layers:

(a) Corporate Governance of ICT – the Governance of ICT through structures, policies and processes.

(b) Governance of ICT – through Standard Operating Procedures.

The difference between the Corporate Governance of ICT and the Governance of ICT can be defined as follows:

Corporate Governance of ICT: *The system by which the current and future use of ICT is directed and controlled.*

Governance of ICT: *The individual processes and procedure which ensure the compliance of the ICT environment based on a pre-agreed set of principles.*

In November 2012, Cabinet approved the Public Service Corporate Governance of ICT Policy Framework and made ICT applicable to National and Provincial Departments, Provincial Administrations, Local Governments, Organs of State and Public Entities for implementation by July 2014.

To address the above mentioned, the Western Cape Department of Local Government in collaboration with the Department of Cooperative Governance (DCOG) , the Department of Public Service and Administration (DPSA), the South African Local Government Association (SALGA), and the Western Cape Provincial Treasury, developed this Municipal Corporate Governance of ICT Policy for application in the Local Government sphere.

The purpose of the Municipal ICT Governance Policy is to institutionalise the Governance of ICT as an integral part of corporate governance within municipalities. This Municipal ICT Governance Policy provides the Municipal Council and Management within a municipality with a set of principles and practices that must be complied with, together with an implementation approach to be utilised for implementation of ICT Governance within Municipalities.

To enable a municipality to implement this Municipal Corporate Governance of ICT Policy, a three-phase approach will be followed:

(c) **Phase 1 – Enabling Environment :** The Corporate Governance of ICT environments will be established in Municipalities through the adoption of this Municipal Corporate Governance of ICT Policy and its associated policies through Council resolution;

(d) **Phase 2 – Business and Strategic Alignment:** Municipalities will plan and implement the alignment between IDP's, strategic goals and ICT strategy.

(e) **Phase 3 – Continuous Improvement:** Municipalities will enter into an on-going process to achieve continuous improvement of all elements related the Governance of ICT.

This Corporate Governance of ICT Policy will allow municipalities to maintain alignment of strategic ICT functions to meet their needs and apply best practices in order to reduce costs and increase the effectiveness of the ICT service delivery to the municipality.

INDEX

Page

GLOSSARY

AG	Auditor-General of South Africa
CMMI	Capability Maturity Model Integration
CIO	Chief Information Officer
CGICTPF	Corporate Governance of ICT Policy Framework
COBIT®	Control Objectives for Information Technology
DPSA	Department of Public Service and Administration
DCOG	Department of Cooperative Governance
ICT	Information and Communications Technology
ISACA®	Information Systems Audit and Control Association
ISO/IEC	International Organisation for Standardisation (ISO) and the International Electro technical Commission (IEC)
ISO/IEC 38500	International Standard on Corporate Governance of ICT (ISO/IEC WD 38500: 2008: 1)
ITGI™	ICT Governance Institute
ITIL	The Information Technology Infrastructure Library
King III	The King III Report and Code on Governance for South Africa
MICTGPF	Municipal ICT Governance Policy Framework
M&E	Monitoring and Evaluation
PSCGICTPF	Public Service Corporate ICT Governance Policy Framework
SALGA	South African Local Government Association
SDBIP	Service Delivery and Budget Implementation Plan

1. ICT GOVERNANCE OVERVIEW

1.1 Introduction

Information and Communications Technology (ICT) Governance has been described as the effective and efficient management of ICT resources to facilitate the achievement of organizational goals and objectives. ICT does not exist for its own sake within an organisation; ICT is there to make sure that organizations achieve sustainable success through the use of their ICT. The ICT Governance Institute describes ICT Governance as, "...the responsibility of the board of directors and executive management. ICT is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's ICT [the infrastructure as well as the capabilities and organisation that is established to support ICT] sustain and extends the organisation's strategies and objectives".

1.1 PURPOSE

The purpose of this policy is to institutionalise the Corporate Governance of ICT as an integral part of corporate governance within municipalities in a uniform and coordinated manner. The policy provides a set of principles and practices which will assist to institutionalise the Corporate Governance of ICT.

1.2 LEGISLATIVE FRAMEWORK

Municipalities must be aware of and comply with the legislative landscape applicable to their context. This includes the Local Government Municipal Systems Act, Act 32, of 2000, Local Government: Municipal Structures Act, Act 117 of 1998, the Public Administration Management Act , Act 11 of 2014 and the Local Government: Municipal Finance Management Act, Act 56 of 2003.

This framework has been developed with following sections of legislation in mind:

a. In terms of the Municipal Systems Act, Act 32, of 2000, Section 55(1):

"the municipal manager of a municipality is, subject to the policy directions of the municipal council, responsible and accountable for:

(a) The formation and development of an economical effective, efficient and accountable administration :

(i) equipped to carry out the task of implementing the municipality's integrated development plan in accordance with Chapter 5:

(ii) Operating in accordance with the municipality's performance Management system in accordance with Chapter 6;"

b. In terms of the Municipal Finance Management Act, Act 56 of 2003, Section 62:

" The accounting officer of a municipality is responsible for managing the financial administration of the municipality, and must for this purpose take all reasonable steps to ensure—

(a) that the resources of the municipality are used effectively, efficiently

and economically;
(b) that full and proper records of the financial affairs of the municipality are kept in accordance with any prescribed norms and standards;"

c. In terms of the Municipal Finance Management Act, Act 56 of 2003, Section 78 of the Municipal Finance Management Act stipulates that:

"Each senior manager of a municipality and each official of a municipality exercising financial management responsibilities must take all reasonable steps within their respective areas of responsibility to ensure—
(a) that the system of financial management and internal control established for the municipality is carried out diligently;
(b) that the financial and other resources of the municipality are utilised effectively, efficiently, economically and transparently;
(c) that any unauthorised, irregular or fruitless and wasteful expenditure and any other losses are prevented;"

1.3 SCOPE

This Policy has been developed to guide and assist Breede Valley Municipality to be aligned with the ICT Governance best practise frameworks.

This Policy therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective Corporate Governance of ICT.

1.4 BENEFITS OF GOOD GOVERNANCE OF ICT

When the Governance of ICT is effectively implemented and maintained, the following benefits are realised:

a. Establishment of ICT as a strategic enabler in a municipality.
b. Improved achievement of municipal integrated development plans;
c. Improved effective service delivery through ICT-enabled access to municipal information and services;
d. Improved ICT enablement of a municipality;
e. Improved delivery of ICT service quality;
f. Improved stakeholder communication;
g. Improved trust between the municipality and the community through the use of ICT;
h. Lower costs (for ICT functions and ICT dependent functions)
i. Increased alignment of ICT investment towards municipal integrated development plans;
j. Improved return on ICT investments;
k. ICT risks managed in line with the ICT priorities and risk appetite of the municipality;
l. Appropriate security measures to protect both the municipality's and its employees information;
m. Improved management of municipal-related ICT projects;

n. Improved management of information as ICT is prioritised on the same level as other resources in municipalities;

o. ICT pro-actively recognises potential efficiencies and guides municipalities in timeous adoption of appropriate technology;

p. Improved ICT ability and agility to adapt to changing circumstances; and

q. ICT executed in line with legislative and regulatory requirements.

1.5 CORPORATE GOVERNANCE OF ICT GOOD PRACTICE AND STANDARDS

In recognition of the importance of ICT Governance, a number of internationally recognised frameworks and standards have been developed to provide context for the institutionalisation of the governance of ICT.

r. The **King III Code:** The most commonly accepted Corporate Governance Framework in South Africa is also valid for Municipalities. ICT was used to inform the Governance of ICT principles and practices and to establish the relationship between Corporate Governance of and Governance of ICT.

s. **ISO/IEC 38500:** Internationally accepted as the standard for Corporate Governance of ICT; ICT provides governance principles and a model for the effective, efficient, and acceptable use of ICT within municipalities.

t. **Other** internationally accepted process frameworks for implementing Governance of ICT.

1.6 LAYERED APPROACH TO CORPORATE GOVERNANCE OF ICT IN MUNCIPALITIES

Corporate Governance of ICT encompasses two levels of decision-making, authority and accountability to satisfy the expectations of all stakeholders. These levels are:

u. Facilitating the achievement of a municipality's strategic goals (Corporate Governance of ICT); and

v. The efficient and effective management of ICT service delivery (Operational Governance of ICT).

The implementation of Corporate Governance of ICT in Municipalities thus consists of the following layered approach:

w. This Municipal Corporate Governance of ICT Policy, which addresses the **Corporate Governance of ICT** layer.

x. Other best practise frameworks which will be adapted to give effect to the governance of the ICT operational environments within municipalities.

1.6.1 CORPORATE GOVERNANCE IN MUNICIPALITIES:

Corporate governance is a vehicle through which value is created within a municipal context. Value creation means realising benefits while optimising resources and risks. This value creation takes place within a governance system that is established by the municipal policy framework. A governance system refers to all the means and mechanisms that enable the municipality's Council and Management team to have a structured and organised process.

1.6.2 CORPORATE GOVERNANCE OF ICT IN MUNICIPALITIES:

The Corporate Governance of ICT is an integral part of the governance system in municipalities. The Corporate Governance of ICT involves evaluating, directing and monitoring the alignment of the municipal ICT strategy with the municipal IDP's and related strategies. The Corporate Governance of ICT also involves the monitoring of ICT service delivery to ensure a culture of continuous ICT service improvements exist in the municipality. The Corporate Governance of ICT includes determining ICT strategic goals and plans for ICT service delivery as determined by the Service Delivery and Budget Implementation Plan (SDBIP) objectives of the municipality.

1.7 MUNICIPAL CORPORATE GOVERNANCE OF ICT POLICY OBJECTIVES

The objectives of this Corporate Governance of ICT Policy seek to achieve the following:

a. Institutionalising a Corporate Governance of ICT Policy that is consistent with the Corporate Governance Frameworks of the municipality;
b. Aligning the ICT strategic goals and objectives with the municipality's strategic goals and objectives;
c. Ensuring that optimum Municipal value is realised from ICT-related investment, services and assets;
d. Ensuring that Municipal and ICT-related risks do not exceed the municipality's 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.

1.8 THE PRINCIPLES FOR THE CORPORATE GOVERNANCE OF ICT:

This Municipal Corporate Governance of ICT Policy is based on principles as explained in international good practices and standard for ICT governance, namely, King III Code, ISO/IEC 38500 and other best practise process frameworks.

Table 1 below contains the principles which have been adopted in the Public Service Corporate ICT Governance Policy Framework (PSCGICTPF) which have been adapted for municipalities.

Principle 1: **Political Mandate** The Governance of ICT must enable the municipality's political mandate.
The Municipal Council must ensure that Corporate Governance of ICT achieves the service delivery mandate of the municipality.
Principle 2: Strategic Mandate The Governance of ICT must enable the municipality's strategic mandate.

The Municipal Manager must ensure that Corporate Governance of ICT serves as an enabler to the municipality's strategic plans.
Principle 3: Corporate Governance of ICT The Municipal Manager is responsible for the Corporate Governance of ICT.
The Municipal Manager must create an enabling environment in respect of the Corporate Governance of ICT within the applicable legislative and regulatory landscape and information security context.
Principle 4: ICT Strategic Alignment ICT service delivery must be aligned with the strategic goals of the municipality.
Management must ensure that ICT service delivery is aligned with the municipal strategic goals and that the administration accounts for current and future capabilities of ICT. ICT must ensure that ICT is fit for purpose at the correct service levels and quality for both current and future Municipal needs are met.
Principle 5: Significant ICT Expenditure Management must monitor and evaluate significant ICT expenditure.
Management must monitor and evaluate major ICT expenditure, ensure that ICT expenditure is made for valid Municipal enabling reasons and monitor and manage the benefits, opportunities, costs and risks resulting from this expenditure, while ensuring that information assets are adequately managed.
Principle 6: Risk Management and Assurance Management must ensure that ICT risks are managed and that the ICT function is audited.
Management must ensure that ICT risks are managed within the municipal risk management practice. ICT must also ensure that the ICT function is audited as part of the municipal audit plan.
Principle 7: Organisational Behaviour Management must ensure that ICT service delivery is sensitive to organisational behaviour/culture.
Management must ensure that the use of ICT demonstrates the understanding of and respect for organisational behaviour/culture.

Table 1: Corporate Governance of ICT Principles

1.9 MUNICIPAL CORPORATE GOVERNANCE of ICT POLICY

The following functions, outlined in Table 2 below, have been assigned to specific designated municipal structures and officials in order to achieve the objectives and principles contained in this Municipal Corporate Governance of ICT Policy:

Practise No.	Practices Description
1.	**The Municipal Council must:** Provide political leadership and strategic direction through, • Determining policy and providing oversight; • 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 municipality to leverage ICT as an enabler the municipal IDP • Assist the Municipal Manager to deal with intergovernmental, political and other ICT-related Municipal issues beyond their direct control and influence; and • Ensure that the municipality's organisational structure makes provision for the Corporate Governance of ICT.
2.	**The Municipal Manager must:** • Provide strategic leadership and management of ICT, • Ensure alignment of the ICT strategic plan with the municipal IDP; • Ensure that the Corporate Governance of ICT is placed on the municipality's strategic agenda; • 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 management; • Determine the delegation of authority, personal responsibilities and accountability to the Management with regards to the Corporate Governance of ICT; • Ensure the realisation of municipality-wide value through ICT service delivery and management of Municipal and ICT-related risks; • Ensure that appropriate ICT capability and capacity are provided and a suitably qualified and experienced Governance Champion is designated. • Ensure that appropriate ICT capacity and capability are provided and that a designated official at a Management level takes accountability for the Management of ICT in the municipality. • Ensure the monitoring and evaluation of the effectiveness of the Corporate Governance of ICT system e.g. ICT steering committee.
3.	**The Municipal ICT Steering Committee, Risk and Audit Committee must:** • Assist the Municipal Manager in carrying out his/her Corporate Governance of ICT accountabilities and responsibilities.

Practise No.	Practices Description
4.	**Management must ensure:** • ICT strategic goals are aligned with the municipality's Municipal strategic goals and support the municipal processes; • Municipal-related ICT strategic goals are cascaded throughout the municipality for implementation and are reported on.

Table 2: Corporate Governance - Functions

2. Practical implementation OF this municipal corporate governance of ict policy.

Upon approval of this Policy, the municipality must approve a Corporate Governance of ICT Charter and practical implementation plan.

2.1 THE CORPORATE GOVERNANCE of ICT CHARTER

The Charter should guide the creation and maintenance of effective enabling governance structures, processes and practices. ICT should also clarify the governance of ICT-related roles and responsibilities towards achieving the municipality's strategic goals.

2.1.1 OBJECTIVES OF THE MUNICIPAL ICT CORPORATE GOVERNANCE CHARTER

In order to give effect to the Corporate Governance of ICT in Municipalities, the following objectives should be included in the municipality's ICT Governance charter:

a. Identify and establish an Corporate Governance of ICT Policy and implementation guideline for the municipality;

b. Embed the Corporate Governance of ICT as a subset of the municipal governance objectives.

c. Create Municipal value through ICT enablement by ensuring municipal IDP and ICT strategic alignment;

d. Provide relevant ICT resources, organisational structure, capacity and capability to enable ICT service delivery;

e. Achieve and monitor ICT service delivery performance and conformance to relevant internal and external policies, frameworks, laws, regulations, standards and practices;

f. Implement the governance of ICT in the municipality, based on an approved implementation plan.

2.1.2 DESIGN OF THE MUNICIPAL CORPORATE GOVERNANCE of ICT CHARTER

This charter should be approved at a strategic level in the municipality and should contain the following:

a. How the ICT strategic goals and their related service delivery mechanisms will be aligned with municipal IDP, monitored and reported on to the relevant stakeholders;

b. How ICT service delivery will be guided at a strategic level to create ICT value in the municipality;

c. How the administrations ICT-related risks will be managed;

d. The establishment of structures to give effect to the Governance of ICT, and the management of ICT functions. The members of these structures and the roles, responsibilities and delegations of each should be defined. The proposed structures are as follows:

STRUCTURE	MEMBERS	MANDATE/RESPONSIBILITIES
ICT STEERING COMMITTEE (Committee of Management)	Designated Members of Management and the ICT Manager. The Chairperson shall be a designated member of the Management of the Municipality duly appointed by the Municipal Manager.	Has a specific delegated responsibility to ensure the planning, monitoring and evaluation, of the municipalities: • ICT structures. • ICT policies. • ICT procedures, processes, mechanisms and controls regarding all aspects of ICT use (Municipal and ICT) are clearly defined, implemented and enforced. • ICT Performance Management. • ICT Change Management. • ICT Contingency Plans. • ICT Strategy development. • Management of ICT Security and Data Integrity. • The establishment of the municipalities ICT Ethical culture. • The evaluation, directing and monitoring of ICT specific projects. • ICT Strategic alignment. • ICT Governance compliance. • ICT Infrastructure Management. • ICT Security. • ICT Application Management. • ICT Value. • ICT Data availability and integrity. • ICT Vendor Management. • The evaluation, directing and monitoring of ICT processes
Audit Committee and Risk Committee	Nominated members of the Audit and Risk committee/s of	Has a specific responsibility to perform an oversight role for the Identification and Management of ICT audit and governance compliance, and ICT Risks.

STRUCTURE	MEMBERS	MANDATE/RESPONSIBILITIES
	the municipality and the ICT Manager or CIO.	

Table 3: ICT Governance roles, responsibilities and delegations

2.2 Municipal IDP and ICT Strategic Alignment

This accountability assigned to the leadership of a municipality through this ICT Corporate Governance Policy Framework enables the municipality to align the delivery of ICT strategies and services with the municipality's Integrated Development Plans and strategic goals.

This is achieved through the development and adoption of an ICT strategic plan which is informed by the enterprise architecture plan which clearly outlined the roles, responsibilities and business processes contained in the IDP.

2.3 CONTINUOUS SERVICE IMPROVEMENT OF ICT IN THE MUNICIPALITY

In this phase, all aspects of the **Corporate Governance of ICT** demonstrate measurable improvement from the initial implementation phase 2016–20. In this phase, detailed measurable criteria for the implementation of and compliance against the approved ICT Corporate Governance Policy and implementation plan are established and can be measured for compliance. In this phase the applicability of all elements of the ICT Corporate Governance Policy Framework is tested for efficacy and efficiency.

2.4 THE DETAILED PHASED APPROACH

Implementation deliverables per financial year

Phase 1 (Enablement Phase): To be completed by June 2017

1) Municipal Corporate Governance of ICT Policy approved and implemented;
2) ICT Governance Charter approved and implemented;
3) The following capabilities created in the municipality:
    - Governance Champion designated and responsibilities allocated;
    - A proficient ICT Manager or CIO appointed functioning at strategic level.
    - Approved and implemented **Risk Management Policy** that includes the management of Municipal-related ICT risks;
    - Approved and implemented **Internal Audit Plan** that includes ICT audits;
    - Approved and implemented **ICT Management Framework**;
    - Approved and implemented municipal **Portfolio Management Framework** that includes ICT portfolio/programme and project management;
    - Approved **ICT Disaster Recovery Plan** informed by Municipal Continuity Plan and Strategy.
    - Approved **Data Backup and Recovery policy**.
    - Approved **ICT Service Level Agreement Management policy**.
    - Approved **ICT User Access Management policy.**

- Approved **ICT Security Controls policy.**
- Approved **ICT Operating System Security Controls policy.**

Phase 2 (Strategic Alignment): to be completed by June 2019

1) Approved **Enterprise Architecture** informing the ICT Architecture;
2) Approved medium term ICT Strategy.
3) Approved **ICT Migration Plan** with annual milestones linked to an enabling budget;
4) Approved **ICT Performance Indicators as contained in the municipality's performance management system**.

Phase 3: Continuous improvement of Corporate Governance of and Governance of ICT

The successful implementation of a Corporate Governance of ICT system leads to continuous improvement in the creation of value to the municipality. ICT delivery must be assessed on an on-going basis to identify gaps between what was expected and what was realised. Assessments must be performed coherently and encompass both:

a) The Corporate Governance of ICT (ICT contribution to realisation of Municipal value); and
b) Governance of ICT. (Continuous improvement of the management of ICT).

3. CONCLUSION

This Corporate Governance of ICT Policy has been designed for the exclusive use and alignment of the Municipality.

INFORMATION & COMMUNICATION TECHNOLOGY
STEERING COMMITTEE CHARTER

Pre-amble

"The Governance of Information and Communications Services and Systems (ICT) is a continuous function that should be embedded in all operations of the municipality: From Executive Authority and Executive Management level and in all Departments. The Corporate Governance of ICT should provide for the necessary strategies, architectures, plans, policies, structures, procedures, processes, mechanisms and controls, and ethical culture."

Change Control History		
Date	**Version**	**Comments**
February 2015	V1	Alignment with WCDLG and DPSA ICT Policy Framework & Guidelines for Governance in Local Government (MCGICTPF)

INDEX

1. BACKGROUND AND PURPOSE

The Department of Public Service and Administration (DPSA) in collaboration with the Government Information Technology Officer Council (GITOC) and the Auditor General Policy Framework was specifically amended to meet the requirements of ICT in local government, and hence the MCGICTPF was established.

This Policy Framework does however, recognize that municipalities are diverse. It is thus not possible to produce a blueprint of an enabling environment applicable to all municipalities. Municipalities must therefore develop their own system of Corporate Governance of ICT by adopting the principles and practices put forward in this Policy Framework and by adapting their governance system to be in line within the municipal context, while keeping the intent of this Policy Framework intact.

The purpose of the MCGICTPF is to institutionalise the Governance of ICT as an integral part of Corporate Governance within Municipalities. *This MCGICTPF provides the Political and Executive Leadership with a set of principles and practices that must be complied with, together with an implementation approach to be utilised for Corporate Governance of ICT within Municipalities.*

(Extracts from the DPSA: Corporate Governance of Information and Communications Technology Policy Framework Published in December 2012 and as amended in June 2013)

2. LEGISLATIVE FRAMEWORK

This charter take cognizance of the legal framework provided for in the following legislations and/or policies of the Municipality and as may be amended from time to time:

- Local Government Municipal Structures Act, No 117, 1998;
- State Information Technology Act, No 88, 1998;
- Local Government: Municipal Systems Act, No 32, 2000;
- Preferential Procurement Policy Framework Act, No 5, 2000;
- Electronic Communications Security Act, No 68, 2002;
- Local Government: Municipal Finance Management Act, No 56, 2003;
- Electronic and Communications Act, No 68, 2005;
- Breede Valley Municipality: Supply Chain Management Policy.

3. INDUSTRY STANDARD ICT FRAMEWORKS

The view that ICT should be governed and managed at a Political Leadership as well as Executive Management level is supported by international accepted good practice and standards in the form of **King III Code** of Good Governance; **ISO 38500 Standard** for the Corporate Governance of ICT; **COBIT,** a comprehensive Governance ICT Process Framework and **ITIL**, a best practice approach to ICT Service Management and to align ICT Services and systems with the needs of business.

4. STRATEGIC OBJECTIVES AND BUSINESS BENEFITS

Once the governance of ICT is successfully integrated with the corporate governance in the municipality the following strategic objectives and business benefits will be achieved:

- Establishing ICT as a strategic enabler of organizational growth;
- Improved understanding that ICT services and systems should be managed on the same level as other departments in the Municipality;
- Improved and cost effective service delivery through ICT-enabled access to municipal information and services;
- Improved achievement of municipality's strategic goals and objectives;
- Improved stakeholder communication;
- Improved strategic alignment between ICT and lines of business;
- Improved trust between ICT, the lines of business and citizens;
- Informed decision making and funding of ICT Initiatives to achieve the strategic goals of the municipality;
- Improved understanding and management of ICT related risks;
- Improved understanding of ICT security measures required to protect the municipal data assets and employee information;
- Improved management of ICT projects in line with municipal priorities;
- Improved ability for the municipality to learn and agility to adapt to changing circumstances; and
- ICT executed in compliance with legislative and regulatory requirements and policy frameworks.

5. RESPONSIBILITIES OF THE ICT STEERING COMMITTEE

5.1 RESPONSIBILITIES OF THE EXECUTIVE LEADERSHIP

The permanent members of the ICT Steering Committee are collectively responsible to execute its mandate within the following guidelines:

ICT Governance and Management:

- Developing and maintaining corporate level ICT strategies and ICT Business Plans that will ensure the cost effective deployment and management of ICT services, systems, facilities and resources throughout the Municipality;
- Ensuring that ICT strategies and Business Plans are aligned with wider municipal directions and priorities as well as the Municipality's strategic and corporate objectives, its Integrated Development Plan and its Service Delivery and Budget Implementation Plan;
- Ensuring that the ICT Business Plan will be delivered within the agreed budget and timeframes;
- Capacitating the Manager: ICT to achieve his/her Departmental objectives;

- Providing the Executive Mayor with regular progress reports on the implementation of the ICT Strategic Plans, new initiatives and projects, as well as advising and recommending on current ICT issues and developments

ICT Projects Planning and Management:

- Ensuring that the Municipality adopts a structured project management methodology;
- Monitoring and evaluating new ICT projects and anticipated achievements against the ICT Strategic Plan;
- Assessing the priorities for all new ICT projects, and resolve competing demands for resources and funding;
- Ensuring that every project proposal and implementation plan will achieve appropriate levels of user and stakeholder consultation and satisfaction;
- Ensuring that all ICT projects have a suitably qualified and responsible person fulfilling the role of Systems Administrator for all business application systems;
- Reviewing ICT project implementation plans and project management reports to assess and mitigate any potential organizational risks and exposure to information security breaches;
- Monitor the implementation of ICT projects against approved project plans, with particular emphasis on quality and the anticipated business benefits to be achieved - Return on investments;

Emerging Technologies:

- Review current and future technologies to identify opportunities to increase the efficiency of ICT services and systems
- Consider new ICT projects that emerge outside the ICT Strategic Planning Cycle and assess the impact and potential business benefits of its implementation on other projects, priorities, budgets etc. in the ICT Strategic Plan;

ICT Systems and Database Architectures:

- Ensuring that the information systems architecture and technology platforms proposed for new projects is consistent with the strategic ICT architectures and plans of the municipality;
- Ensuring that proper integration of ICT systems within the Municipality of all current and new systems is achievable via an approved ICT Systems architecture and an approved ICT Infrastructure architecture;

5.2 RESPONSIBILITIES OF THE MANAGER: ICT

The Manager: ICT is the Head of the Municipal ICT Division and should have access to and regularly interact on strategic ICT matters with the Director: Strategic and Corporate Services.

He / She is expected to report to the Director: Strategic and Corporate Services about the effective and efficient management of IT resources to facilitate the achievement of the strategic objectives and goals of the Municipality.

King III requires the ICT Manager to define, maintain and validate the ICT value proposition; align ICT activities with sustainable ICT objectives and solutions; implement an ICT control framework to ensure all parties in the value chain, from procurement to

deployment of ICT Services and Systems, apply good governance principles, in compliance with the relevant legislative and regulatory compliance requirements.

Other functions of the ICT Manager include:

Develop and Maintain **the Annual ICT Business Plan** to ensure that the deployment of ICT Services and system will remain align with the strategic goals and objectives of the municipality;
Develop and maintain an **ICT Service Delivery Framework (ISDF)** based on the COBIT and ITIL principles. This ISDF is to ensure:

i. Ensure the continuous existence and support to the ICT Steering Committee;
ii. Ongoing awareness between ICT and lines of business of emerging technologies and trends, and
iii. Continued collaboration between ICT, lines of business and other stakeholders in the deployment of ICT initiatives in line with Departmental Business Implementation Plans;

Refer paragraph 8 to this ICT Charter for a schematic presentation of the ICT Service Delivery framework;

- Develop and establish appropriate **ICT policies and procedures** to ensure a quality and sustainable ICT service delivery in compliance with the relevant legislative and regulatory requirements, and in line with best practice industry standards;

- Pro-actively **recognise opportunities for change** and guides Municipalities in timeous adoption of appropriate technologies;

- Manage the **relationships between all stakeholders** in the rendering of ICT related services;

- **Co-management of all contracts** for ICT related services and systems to ensure financial and technical transparency and that value for money is achieved at all times;

- **Service Level Management** – Vendor performance monitoring with penalties for non-performance. Advise and recommend to the ICT Steering Committee should the termination of existing contract be considered;

- **Change Management** – Only planned and tested changes are allowed; Mitigation of operational and financial risks;

- **Problem Management** and corrective measures – prevent re-occurrences and trend analysis of all service failures events;

- Manage all **ICT related service requests and Projects** making use of best practice project management methodologies.

6. MEMBERSHIP OF THE ICT STEERING COMMITTEE

The ICT Steering Committee shall include the following permanent members:

a) Executive Mayor (Ex- officio)

b) Municipal Manager (Chairperson)

c) Directors of all the respective Directorates in the Municipality

d) Two or more full time Councillors as nominated by the Executive Mayor;

e) Manager: ICT Services and Systems

f) ICT Business Analyst (when appointed)

g) Chief Risk Officer

h) Chief Internal Auditor (ex-officio)

i) Manager: IDP

Any other official/s the Municipal Manager may deem necessary to be a permanent member of this meeting.

Alternative members may be co-opted to attend the ICT Steering Committee meeting at the discretion of their respective Directors and the prior approval of the Chairperson.
The Chairperson may also invite other persons to attend meetings as required.
In the absence of a permanent member his/her delegate may attend the meeting on behalf of the member.

In the absence of the chairperson, the members shall amongst themselves elect acting chairperson to chair the meeting.

7. COMMITTEE MEETINGS AND CONDUCT

- The Chairperson must at all times be notified of absence of leave by permanent members prior to the meeting;
- The Chairperson, or his delegated official, must approve the Agenda for all meetings, prior to the meeting taking place;
- Decisions and resolutions taken at meetings will be noted and the minutes will be distributed to committee members not later than seven working days after the meeting. Secretarial support will be provided for this purpose;
- The quorum for meetings will be a simple majority of the permanent members;
- The ICT Steering Committee must meet at least once every quarter. or at least four times a year;
- Written notice of committee meetings and the minutes of the last meeting must be circulated to all members at least 7 (seven) days prior to a meeting.
- The Director; Strategic and Corporate Services, will nominate a meeting coordinator to provide the required administrative support and to keep the minutes of the meetings.
- The ICT Steering Committee shall report directly to the Executive Mayor.

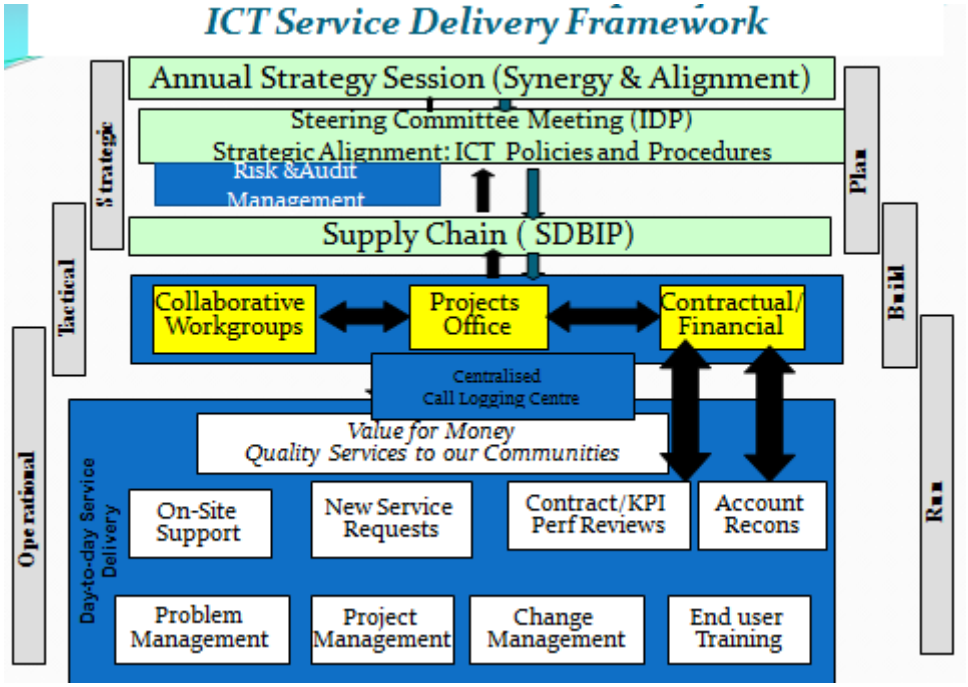
8. ICT SERVICE DELIVERY FRAMEWORK

The MICTCGPF requires that an ICT Service Delivery Framework (ISDF), based on COBIT and ITIL principles, be established and maintained by the ICT Division to:

- Enable a seamless and transparent integration between corporate governance in local government and all ICT related Services and Systems, being the ICT Steering Committee and the ICT Steering Committee Charter;
- Provide a framework for the execution of the Annual ICT Business Plan in compliance with all the relevant regulatory requirements as well as all the relevant policy frameworks in the municipality.

All applicable forum mandates and communication structures must be approved and authorized by the ICT Steering Committee to give full effect to the execution of the Annual ICT Business Plan.

The ICT forums and its mandates are documented and maintained in the ICT Service Delivery Framework.



9. GLOSSARY OF TERMS AND DEFINITIONS

AG	Auditor-General of South Africa
Business	The business of the municipality refers to the municipality's service delivery and internal support activities
CGICTPF	Corporate Governance of ICT Policy Framework
COBIT®	internationally accepted process framework for implementing Governance of ICT. COBIT fully supports the principles of the King III Code and the ISO/IEC 38500 standard in the Corporate Governance of ICT.
Corporate	A group of related components that enables a municipality to achieve its strategic mandate.
Corporate Governance	"...*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)
Corporate Governance of ICT	Corporate governance of ICT involves evaluating and directing the use of ICT to support the organization, and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organization. (ISO/IEC 38500: 2008: 3)
Department	For the purpose of the MCGICTPF reference to department includes public administration in all spheres of government, organs of state and public enterprises as per Section 195 of the Constitution, Act No 108 of 1996, as amended; it specifically refers to the departments of a municipality, also referenced as Directorates in the municipalities.
DPSA	Department of Public Service and Administration
Electronic Government	The use of information and communication technologies in the Public Service to improve its internal functioning and to render services to the public
EXCO	Executive Committee (consists of Executive Management members of a municipality)
Executive Authority	According to section 11(1) of the Municipal Systems Act (Act 32 of 2000) the executive and legislative authority of a municipality is exercised by the council of the municipality. Executive Authority means Executing Authority In a Constitutional Institution: The Chairperson of the Constitutional Institution in relation to a Constitutional Institution with a body of persons, and in relation to a Constitutional Institution with a single office bearer, the incumbent of that office;
Executive Management	Executive Management includes the Municipal Manager and the Managers directly accountable to the Municipal Manager (See sections 56 and 57 of the Municipal Systems Act, No 32 of 2000.).
GICT	Governance of ICT

GITO	Government Information Technology Officer (Cabinet Memorandum 38(a) of 2000)
GITOC	Government Information Technology Officer's Council (Cabinet Memorandum 38(a) of 2000)
Governance Champion (GC)	The Senior Manager in the municipality who is responsible to drive Corporate Governance of and Governance of ICT.
Governance of ICT	The effective and efficient management of ICT resources to facilitate the achievement of company strategic objectives. (King III Code: 2009: 52) The system by which the current and future use of IT is directed and controlled.
Governance Principles	The vehicle to translate the desired behaviour into practical guidance for day-to-day management (COBIT 5 Framework Exposure Draft: 29)
ICT	Information and Communications Technology also referred to as IT.
ISACA®	Information Systems Audit and Control Association
ISO/IEC	International Organization for Standardization (ISO) and the International Electro technical Commission (IEC)
ISO/IEC 38500	An Internationally accepted Standards and principles on Corporate Governance of ICT (ISO/IEC WD 38500: 2008: 1)
ITIL	The Information Technology Infrastructure Library is a set of best practices for ICT service management that focuses on aligning ICT services with the needs of business
King III	The most commonly accepted Corporate Governance Framework in South Africa is also valid for Municipalities. It was used to inform the Corporate Governance of ICT principles and practices in this document and to establish the relationship between Corporate Governance of and Governance of ICT.
MCGICTPF	Municipal Corporate Governance of ICT Policy Framework

ICT SECURITY CONTROLS POLICY

TABLE OF CONTENTS

Glossary of Abbreviations

Abbreviation	Definition
BYOD	Bring Your Own Device
COBIT	Control Objectives for Information and Related Technology
ICT	Information and Communication Technology
IP	Internet Protocol
ISO	International Organization for Standardisation
ODBC	Open Database Connectivity
PIN	Personal Identification Number
SSH	Secure Shell
UPS	Uninterrupted Power Supply
USB	Universal Serial Bus
WPA2	Wi-Fi Protected Access 2

Glossary of Terminologies

Terminology	Definition
Administrative rights	Access rights that allow a user to perform high level/administrative tasks on a device/application such as adding users, deleting log files, deleting users.
Biometric information	Personal information obtained through biometric measurements, such as finger prints, retina, DNA, etc.
Internal system processes	Processes that are performed by the system with no human intervention. Part of the internal working of the system or application.

1. INTRODUCTION

Information security is becoming increasingly important to the Municipality, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that the Municipality's ICT systems, data and infrastructure are protected from risks such as unauthorised access (see ICT User Access Management Policy for further detail), manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

2. LEGISLATIVE 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:

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996.
- 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 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
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- King Code of Governance Principles, 2009

3. OBJECTIVE OF THE POLICY

The objective of the policy is to reduce the risk of harm that can be caused to the Municipality's ICT systems, information and infrastructure. This policy also seeks to outline the acceptable use of ICT resources by Officials and 3rd party service providers, to ensure that the investment in modern technology is applied to the best advantage of the Municipality.

This policy defines the collective controls to prevent Information Security related risk from hampering the achievement of the Municipality's strategic goals and objectives.

4. AIMS OF THE POLICY

The aim of this policy is to ensure that the Municipality conforms to a standard set of security controls for information security in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that risks associated to the management of Information Security are mitigated. This policy supports the Municipality's Corporate Governance of ICT Policy.

5. SCOPE

This ICT Security Controls Policy has been developed to guide and assist municipalities to be aligned with internationally recognised best practice ICT Security Controls. This policy recognizes that municipalities are diverse in nature, and therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of information security.

The policy applies to everyone in the Municipality, including its 3rd party service providers and consultants.

This policy is regarded as being critical to the security of ICT systems of the Municipality.

Municipalities must develop their own Security controls and procedures by adopting the principles and practices presented in this policy.

The policy covers the following elements of information security:

- Ownership and classification of information;
- Security incident management;
- Physical security;
- Application security;
- Network security;
- Database security;
- Change control; and
- Software authorisation and licensing.

Aspects relating to user access, server security and data backup are covered in the ICT User Access Management, ICT Operating System Security Controls and the ICT Data Backup and Recovery policies.

6. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the Municipality and evaluated on its level of severity.

The appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy. Actions include, but are not limited to:

- Revocation of access to Municipal systems and ICT services;
- Disciplinary action in accordance with the Municipal policy; or
- Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978).
- Punitive recourse against a service provider in terms of the contract.

7. ADMINISTRATION OF POLICY

The ICT Manager or delegated authority is responsible for maintaining the policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and any changes approved by Council.

8. PROTECTION OF CLASSIFIED INFORMATION

8.1 The Municipal Systems Act, Act No. 32 of 2000, Schedule 1: Code of Conduct for Councillors and Schedule 2: Code of Conduct for Municipal Staff Members require Councillors and Officials to employ a strict level of self-discipline in order to prevent communication of sensitive or classified information. Councillors and Officials may not disclose any privileged or confidential information to an unauthorised person.

8.2 All Municipal data must be classified in accordance with the Minimum Information Security Standards, as approved by Cabinet in 1996. Therefore all official matters requiring the application of security measures must be classified either as "Restricted" or "Confidential". By default, Municipal data has been classified as Restricted.

Classification	Description
Restricted	Information that may be used to hamper Municipal activities.
Confidential	Information that may be used harm the objectives and functions of the Municipality.

Table 4: Data classification in accordance with the MISS

8.3 Access to classified information is determined either by the level of security clearance, or if the information is required in the execution of their duties.

8.4 Officials, in conjunction with the ICT Manager, must ensure that classified information receives adequate protection to prevent compromise.

8.5 Officials who generate sensitive information are responsible for determining the information classification levels. This responsibility includes the labelling of classified documents.

8.6 The Minimum Information Security Standards Chapter 6, Section 1 requires that a declaration of secrecy must be made on an official form during the appointment process for any government post.

9. PROTECTION OF PUBLIC RECORDS

9.1 The National Archives and Records Service of South Africa Act, Act 43 of 1996 requires sound records management principles to be applied to electronic records and e-mails created or received in the course of official business and which are kept as evidence of the Municipality's functions, activities and transactions. The detail of these requirements can be found in:

(a) The [Records Management Policy], [Internet and e-Mail Usage], [Web Content Management Policy] and [Document Imaging Policy] of the Municipality; and

(b) The National Archives and Records Service of South Africa Regulations.

9.2 The Records Manager is responsible for the implementation of sound records management principles and record disposal schedules for the Municipality.

9.3 The ICT Manager must work with the Records Manager to ensure that public records in electronic form are managed, protected and retained for as long as they are required.

9.4 Information security plays an important role in records management as a means to protect the integrity and confidentiality of public records. The ICT Manager must ensure that systems used for records management of electronic public records and e-mails are configured and managed as follows:

(a) Systems must capture appropriate metadata (background and technical information about the data);

(b) The systems must establish an audit trail to log all attempts to alter or edit electronic records and their metadata;

(c) The system must protect the integrity of records until they have reached their approved retention. Integrity of records can be accomplished through procedures such as backup test restores, media testing, data migration controls and capturing the required audit trails;

(d) Access controls must protect records against unauthorized access and tampering;

(e) Access controls must prevent removal of data from premises without the explicit permission of the ICT Manager;

(f) Systems must be free from viruses;

(g) The system must ensure that electronic records, that have to be legally admissible in court and carry evidential weight, are protected to ensure that they are authentic, not altered or tampered with, auditable and produced in systems which utilise security measures to ensure their integrity.

(h) Access to server rooms and storage areas for electronic records media must be restricted to ICT staff with specific duties regarding the maintenance of the hardware, software and media.

(i) Systems technical manuals and systems procedures manuals must be designed for each system.

(j) A systems technical manual include information regarding the hardware, software and network elements that comprise the electronic record keeping system and how they interact. Details of all changes to a system must also be documented.

(k) A system procedures manual include all procedures relating to the operation and use of the system, including input to, operation of and output from the system. A systems procedures manual should be updated when new releases force new procedures.

(l) The ICT Manager must ensure that the suitability of new system for records management is assessed during its design phase. The Records Manager must be involved during the design specification.

10. PROTECTION OF PERSONAL INFORMATION

10.1 The Bill of Rights in the Constitution states that the public has a right to privacy, as well as a right to access personal information held by the Municipality.

10.2 The Promotion of Access to Information Act, Act No. 2 of 2000, gives effect to the right to access personal information held by the Municipality and must be complied with.

10.3 The Protection of Personal Information Act, Act No. 4 of 2013, gives effect to the right to privacy. The Act requires that the Information Officer of the Municipality ensure that personal information are lawfully obtained and processed.

10.4 The ICT Manager and Officials must work together to ensure the following with respect to personal information (only key points of the Act included):

(a) Identify the systems and locations where personal information can be found;

(b) Ensure that Municipal policies, in particular those that deal with information security, are applied to the systems and locations where personal information is collected, processed and disposed of;

(c) Put in place business process controls to ensure that personal information are collected lawfully, is complete and accurate, and updated where necessary;

(d) Dispose of excessive personal information, after consultation with the Records Manager;

(e) Put in place structures and systems to allow the access of persons to their personal information stored by the Municipality. The requester may request to have their personal information deleted or corrected if it is incorrect or obtained unlawfully; and

(f) Ensure that systems do not use personal information as the sole basis to decide legal consequences for a person or group of persons (referred to as "automated decision making").

10.5 The Protection of Personal Information Act, No. 4 of 2013, Section 6, contains certain general exceptions where the Act does not apply e.g. the processing of personal information for national security, defence, public safety, law enforcement or for the judicial functions of a court.

10.6 The Protection of Personal Information Act, No. 4 of 2013 prohibits the processing of certain categories of special personal information. The general exception is where a competent person (e.g. in the case of children) have given consent, or if an exception apply. Examples are shown hereunder (refer to the Act for further detail):

Sections	Special personal information	Collection and processing prohibited unless exceptions apply. Examples of exceptions provided:
Sections 6, 34 to 37	Children's information	Establishment or protection of a right of the child.
Sections 6 & 28	Religious or philosophical beliefs	To protect the spiritual welfare of a community.
Sections 6 & 29	Race or ethnic origin	Protection from unfair discrimination or promoting the advancement of persons.
Sections 6 & 30	Trade union membership	To achieve the aims of trade union that the person belongs to.
Sections 6 & 31	Political persuasion	To achieve the aims of a political institution that the person belongs to.
Sections 6 & 32	Health or sex life	Provision of healthcare services, special support for pupils in schools, childcare or support for workers.
Sections 6 & 33	Criminal behaviour or biometric information	Necessary for law enforcement.

Figure 1 : Special personal information protected by the

Protection of Personal Information Act, No. 4 of 2013

10.7 The following personal information are not regarded as special personal information and must be protected in terms of the general rules for the protection of personal information:

Gender, sex, marital status, age, culture, language, birth, education, financial, employment history, identifying number, symbol, e-mail address, physical address, telephone number, location, online identifier, personal opinions, views, preferences, private correspondence, views or opinions about a person, or the name of the person if the name appears next to other personal information or if the name itself would reveal personal information about the person.

10.8 The Promotion of Access to Information Act, Act No. 2 of 2000, prohibits the disclosure of certain types of information held by the Municipality, including, but not limited to personal information. These include:

- Commercial information of a third party;
- Information that falls under a confidentiality agreement;
- Information that is likely to endanger the safety of individuals if it is made public;
- Police dockets in bail proceedings;
- Records privileged from production in legal proceedings;
- Research information of a third party;
- Security information about a building, structure or system;
- Methods, techniques, procedures or guidelines for law enforcement and legal proceedings;
- Information that will prejudice the defence, security and international relations of the Republic;
- Information that will jeopardise the economic interests and financial welfare of the Republic and commercial activities of the Municipality;
- Research information of the Municipality; and
- Information about the operations of the Municipality.

10.9 The Promotion of Access to Information Act, Act No. 2 of 2000, require that information relating to public safety, environmental risk, or a substantial contravention of, or failure to comply with the law, be disclosed immediately.

11. PROTECTION OF RECORDS TO PRESERVE LEGALITY

11.1 The Electronic Communications and Transactions Act, Act. No. 25 of 2002, prescribes information security controls to preserve the evidential weight of electronic records and e-mails.

11.2 The evidential weight of electronic records and e-mails is a continuum, where the weight of the evidence increases with the number of information security controls applied. The following lists examples of such specific information security controls:

- Restrict access to records
- Encrypt records
- Store records on write once, read many times, media

- Apply records management principles
- Store records in a database management system
- Apply change control to the records management system
- Backup data
- Use digital certificates to confirm the identities of senders and receivers of messages

12. GENERAL CONTROL ENVIRONMENT

12.1 To ensure reliability of ICT services and to comply with legislation, all Municipal systems and infrastructure must be protected with physical and logical security measures to prevent unauthorised access to Municipal data.

12.2 Physical and logical security is a layered approach that extends to user access, application security, physical security, database security, operating system security and network security.

12.3 Refer to the ICT User Access Management Policy and the ICT Operating System Security Controls Policy for the requirements relating to user access, applications and operating system security.

13. PHYSICAL SECURITY

13.1 The ICT Manager must take reasonable steps to protect all ICT hardware from natural and man-made disasters to avoid loss and ensure reliable ICT service delivery. ICT hardware under control of the ICT function must be hosted in server rooms or lockable cabinets. Server rooms must be of solid construction and locked at all times.

13.2 The ICT department must retain an access control list for the server room. Access must be reviewed quarterly by the ICT Manager.

13.3 All server rooms must be equipped with air-conditioning, UPS and fire detection and suppression.

13.4 A maintenance schedule must be created and maintained for all ICT hardware under the control of the ICT department. Maintenance activities must be recorded in a maintenance register.

13.5 Server rooms must be kept clean to avoid damage to hardware and reduce the risk of fire.

13.6 Cabling must be neat and protected from damage and interference.

13.7 No ICT equipment may be removed from the server room or offices without prior authorisation from the ICT Manager.

13.8 Officials of the Municipality must be made aware of the acceptable use of ICT hardware.

13.9 All hardware owned by the Municipality must be returned by employees and service providers when no longer needed or on termination of their contract.

13.10 All data and software on hardware must be erased prior to disposal or re-use.

13.11 Any hardware that carry data that can be carried off-site (e.g. laptop computers, removable hard disks, flash drives etc.) must be protected with encryption.

13.12 ICT hardware and software must be standardised as far as possible to promote fast, reliable and cost-effective ICT service delivery to the Municipality.

13.13 The off-site location, used to store backup data media, must be protected with the following physical security measures:

- Building of solid construction;
- Physical access control;
- Fire detection and suppression; and
- Environmental conditions adhere to vendor recommendations for storage of media.

14. DATABASE SECURITY

14.1 The ICT Manager must limit full access to databases (e.g. sysadmin server role, db_owner database role, sa built-in login etc.) to ICT staff who need this access. Officials who use applications may not have these rights to the application's databases.

14.2 The ICT Manager must ensure that Officials who access databases directly (e.g. through ODBC) only have read access.

14.3 The ICT Steering Committee must approve all instances where Officials have edit or execute access to databases.

14.4 The ICT Manager must review database rights and permissions on a quarterly basis. Excessive rights and permissions must be removed.

15. NETWORK SECURITY

15.1 The ICT Manager must document the network structure and configuration including IP addresses, location, make and model of all hubs, switches, routers and firewalls.

15.2 The ICT Manager must implement a firewall between the Municipal network and other networks.

15.3 The ICT Manager must limit administrator access to the firewall and user accounts must have strong passwords of at least 8 characters with a combination of alpha-numeric characters and symbols. Remote firewall administration is only allowed using SSHv2 from the internal network.

15.4 The ICT Manager must check and install firewall upgrades and patches on a weekly basis. An obsolete firewall (one that is not supported by the vendor any longer and / or has known security vulnerabilities) must be replaced.

15.5 The ICT Manager must document the firewall rulesets and configuration settings. The rulesets and configuration settings must be reviewed quarterly to ensure that it remains current (i.e. remove unused services) and that services that expose the Municipality to security risk are reviewed continuously.

15.6 The ICT Manager must configure the firewall to block all incoming ports, unless the service is required to connect to a server on the internal network (e.g. port 80 and port 443 for web servers). When an incoming port is allowed, the service may only connect to the specific servers on the internal network. Internal IP addresses may not be visible outside of the internal network.

15.7 The ICT Steering Committee must approve all open incoming ports. The ICT Steering Committee must only approve requests that are absolutely necessary and with consideration of the associated security risks.

15.8 The system administrators must set the firewall to block intrusion attempts and to alert the ICT Manager when additional action needs to be taken. The ICT Manager must raise an incident and deal with the root causes of the event.

15.9 The ICT Manager must place infrastructure, user devices (e.g. personal computers) and servers facing externally on separate network domains.

15.10 The ICT department must scan the entire network with security software on a monthly basis to detect security vulnerabilities. The scans must be performed from the Internet, as well as from the internal network.

15.11 Officials and the ICT Manager must remove all modems from the internal network to avoid intruders bypassing the firewall.

15.12 System administrators must install personal firewalls on laptops and personal computers. Officials may not disable these firewalls. Officials must choose to deny a specific address when prompted by the personal firewall, unless approved by ICT.

15.13 The ICT department must ensure that all inactive network points are disabled.

16. E-MAIL AND INTERNET

16.1 The ICT Manager must make all users aware of the safe and responsible use of e-mail and Internet services. E-mail and Internet should only be used for official use. Personal usage can be permitted if it does not interfere with job functions. E-mail and Internet may not be used for any illegal or offensive activities.

16.2 Officials and the ICT department may not use Internet cloud services (e.g. Google drive, Gmail, Dropbox etc.) for official purposes unless approved by the ICT Steering Committee.

17. WIRELESS NETWORKS

17.1 System administrators must configure all wireless networks to the following standard:

- WPA2 security protocol or better;
- Password strength of at least 8 characters with a combination of alpha-numeric characters and symbols;
- The latest firmware must be installed; and
- Default system usernames and passwords must be removed.

17.2 Officials may not establish wireless networks attached to the internal network without the consent of the ICT Manager. All wireless networks must adhere to the secure configuration standard.

18. MOBILE DEVICES AND OWN HARDWARE (BYOD)

18.1 The ICT Manager must approve all hardware and software, owned by Officials and service providers, which is to be used for official purposes.

18.2 The ICT team must ensure that all mobile devices must be protected with a PIN.

19. TRANSFER OF INFORMATION

19.1 The ICT Manager must ensure that classified information may only be transmitted over external networks using encryption.

19.2 Officials may not use personal storage devices (e.g. USB memory sticks or portable hard drives) to store Municipal data. When required for official purposes, and the data is of a confidential nature, these devices must be encrypted by the ICT Manager.

20. MONITORING

20.1 The Municipal Manager authorises the monitoring of Municipal systems by the ICT Manager.

20.2 Municipal officials must be made aware that the network is being monitored to ensure network security, to track the performance of the network and systems, and to protect the network from viruses.

20.3 If users give their written consent, any e-mail, Internet and other network service may be monitored. A signed acceptable user agreement is required in order to achieve this consent.

21. SECURITY INCIDENT MANAGEMENT

21.1 All Municipal users must report actual or suspected security breaches or security weaknesses to the ICT Manager or the delegated authority.

21.2 The ICT Manager must record all information regarding security incidents. The ICT Manager must review all the information security incidents on a quarterly basis to ensure that the root cause of the problems are addressed.

21.3 Investigations into security incidents may only be carried out by the ICT Manager or a nominated person.

21.4 The Protection of Personal Information Act, Act No. 4 of 2013 prescribe that the Regular and the person affected by the breach must be notified in the event of a breach of personal information.

22. CHANGE CONTROL

22.1 All changes to Municipal applications and infrastructure must be managed in a controlled manner to ensure fast and reliable ICT service delivery to the Municipality, without impacting the stability and integrity of the changed environment.

(a) Corrections, enhancements and new capabilities for applications and infrastructure will follow a structured change control process.

(b) An emergency change must follow a structured change control process, but with the understanding that documentation must be completed afterwards. Emergency changes are only reserved for fixing errors in the production environment that cannot wait for more than 48 hours.

(c) Recurring change requests from users (e.g. user access requests, a password reset, an installation, move or change of hardware and software etc.) must follow the help-desk processes designed to deliver ICT services in the most effective way.

(d) Recurring operational tasks are excluded from the structured change control process.

22.2 The ICT Manager must establish the formal change control process. Refer Appendix B, Change Control Process.

22.3 The following additional rules with respect to change control must be adhered to. In some cases this may not be cost-effective or technically possible, in which case it is the duty of the ICT Steering Committee to review and approve alternative controls:

(a) The same person who performs the change may not implement the change.

(b) Systems must have a development environment where testing is conducted to avoid testing in the production environment.

(c) If a vendor performs the change, the Municipality must also test the change.

(d) The data inside a database may not be edited, except through an approved application front-end. This excludes internal system processes or interfaces, or work required to convert data during a system implementation.

(e) Commercial software must be selected after considering information security requirements.

(f) The affected user's willingness to change must always be considered when documenting all that can go wrong with the change.

(g) Any system published to the Internet or on a mobile platform must reviewed by security specialists before being deployed.

22.4 The ICT Manager must record all change requests across the Municipality in a central tool, file server or spreadsheet. This implies that changes performed by ICT and those changes requested by the business from vendors, without ICT involvement, must be recorded together.

22.5 The ICT Manager must create a weekly report which lists all of the unapproved change requests, active changes requests, cancelled change requests and completed change requests. The report must be reviewed, and actions taken, to ensure that:

- Change requests receive sufficient attention;
- The change control process is being followed for all known changes; and
- Trends across change requests, that indicate systemic problems in the ICT environment, are identified and require more permanent fixes.

23. SOFTWARE AUTHORISATION AND LICENSING

23.1 The ICT Manager must retain a record of all licenses owned by the Municipality.

23.2 The ICT Manager must scan all ICT resources on an annual basis to verify that only authorised software is installed.

23.3 The ICT Steering Committee must approve all software being used in the Municipality. An approved software list must be maintained by the ICT Manager and approved by the ICT Steering Committee.

23.4 The ICT Steering Committee may only authorise software from known, reputable sources to reduce the likelihood of introducing errors or security risks into the environment.

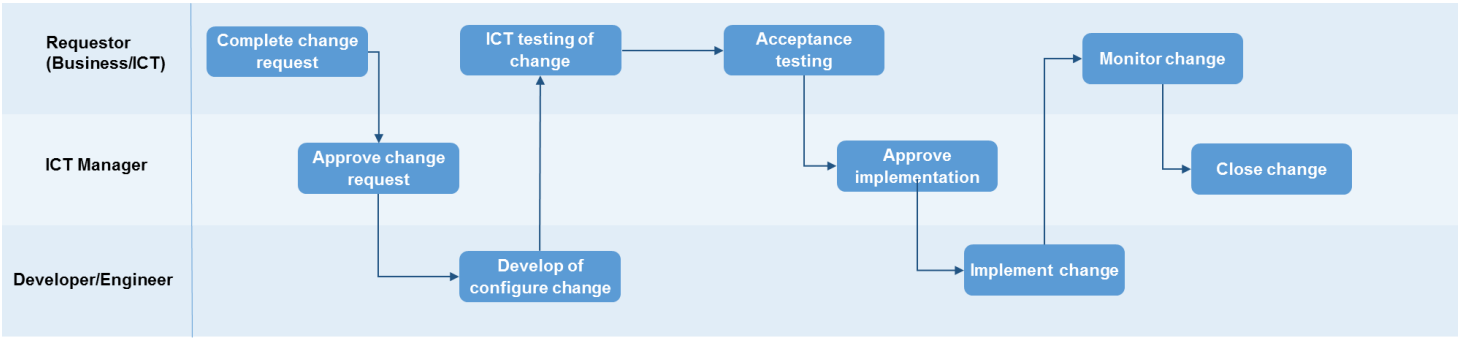
23.5 Officials may not install or change the software on their computers.

24. ANNEXURE A: IMPLEMENTATION ROADMAP

No	Action	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Month 11	Month 12
1	Allocate the information security role												
2	Create an inventory of information that require protection												
3	Perform a gap analysis against the controls in the policy												
4	Create Acceptable Use Policy for IT												
5	Obtain approval from ICT Steering Committee for improvements												
6	Provide security awareness												
7	Implement change control												
8	Implement server room security												
9	Implement user hardware / software use controls												
10	Implement database security												
11	Implement network security												
12	Implement e-mail and Internet security												
13	Implement wireless security												
14	Implement mobile device security												
15	Implement information transfer controls												
16	Implement software licensing												
17	Implement security incident management												
20	Commence operational security management												

25. ANNEXURE B: CHANGE CONTROL PROCESS

25.1 The diagram below depicts the structured change control process:



The structured change control process must include the following steps:

Step	Description
1. Complete change request	Complete a change request (electronic or paper-based). The change request form must include the following information: • A unique number, which runs in a sequence. • Who requested the change. • Who approves the change. • A description of the change in business terms. • A description of the change translated from business terms into specific ICT components that will be changed. • The cost and resources required to perform the change. • All that can go wrong with the change. • What must be done to avoid all that can go wrong. • Roll back plans
2. Approve change request	Seek approval of the change request from the requester and record this on the change request.
3. Develop or configure change	Develop or configure the change to the point where it is ready for testing.
4. ICT testing of change	Test the change from a development or configuration perspective, paying particular attention to prevent all that can go wrong with the change.
5. Acceptance testing	Requester to test the change to determine if the requirement has been met. Pay attention to prevent all that can go wrong with the change.
6. Approve implementation	Seek approval from the requester to implement the change request, and record this on the change request.

Step	Description
7. Implement the change	Implement the change.
8. Monitor the change	Monitor the change for a period of time to ensure that it was successful.
9. Close the change	Seek approval from the requester to close the change request, and record this on the change request.

Table 5 : Change control process, step by step

26. ANNEXURE C: REFERENCES

BS ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls. (2013). Geneva: BSI Standards Limited.

Constitution of the Republic of South Africa. (1996). Republic of South Africa.

Control Objectives for Information Technology (COBIT) 5. (2012). Illinois: ISACA.

Copyright Act No. 98. (1978). Republic of South Africa.

King Code of Governance for South Africa. (2009). Institute of Directors in Southern Africa.

Local Government: Municipal Finance Management Act, No. 53. (2003). Republic Of South Africa.

Local Government: Municipal Structures Act 117. (1998). Republic of South Africa.

Local Government: Municipal Systems Act 32. (2000). Republic of South Africa.

Minumum Information Security Standards. (1996, December 4). Cabinet.

Promotion of Access to Information Act 2. (2000). Republic of South Africa.

Protection of Personal Information Act, No. 4. (2009). Republic of South Africa.

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70. (2002). Republic of South Africa.

ICT USER ACCESS MANAGEMENT POLICY

TABLE OF CONTENTS

Glossary of Abbreviations

Abbreviation	Definition
BYOD	Bring Your Own Device
COBIT	Control Objectives for Information and Related Technology
HR	Human Resources
ICT	Information and Communication Technology
ID	Identifier
ISO	International Organization for Standardisation
ODBC	Open Database Connectivity
PIN	Personal Identification Number
RAS	Remote Access Service
VPN	Virtual Private Network

Glossary of Terminologies

Terminology	Definition
Administrative rights	Access rights that allow a user to perform high level/administrative tasks on a device/application such as adding users, deleting log files, deleting users.
Bring Your Own Device	The practice of allowing employees to use their own devices, such as cell phones, tablets, laptops, or other devices for work purposes.
Business case	A formal requirement in order for a specific business function to perform its required task.
Clear text	Clear text refers to a message that has not been encrypted in anyway and can be intercepted and read by anyone.
COBIT	A best practice framework created by ISACA for Information Technology Management and IT Governance.
Dormant account	A user account that has not been accessed or used for 60 days or more.
Line manager	Each department (HR, Finance, ICT, etc.) should have a manager employed to perform managerial tasks.
Personal Identification Number	A number allocated to an individual and used to validate electronic transactions.
Principle of least privilege	A user or a program must be able to access only the information and resources that are necessary for its legitimate purpose.
Remote Access Service	A service which allows for a user to connect to a remote machine from any network point, as long as the targeted device resides on the network.
Segregation of duties	The principle of dividing a task up based on varying levels of authority in order to prevent fraud and error by requiring more than one person to complete a task.

Terminology	Definition
VPN	A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organisation's network.
Wi-Fi	Wi-Fi is a wireless networking technology that allows computers and other devices to communicate over a wireless signal.

27. INTRODUCTION

Information security is becoming increasingly important to the Municipality, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

28. LEGISLATIVE FRAMEWORK

The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

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

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
- 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;
- 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; and
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following internationally recognised ICT 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;
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls; and
- King Code of Governance Principles, 2009.

29. OBJECTIVE OF THE POLICY

The objective of the policy is to define the user access management control measures for the Municipality's ICT systems, information and infrastructure where it would apply to both the Municipal users and Service Providers.

This policy seeks to further ensure that it protects the privacy, security and confidentiality of the Municipality's information.

The main objective of this policy is to provide the Municipality with best practice User Access Management controls and procedures to assist the Municipality in securing their user access management procedure.

30. AIM OF THE POLICY

The aim of this policy is to ensure that the Municipality conforms to standard user access management controls in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that risks associated to the management of user access are mitigated. This policy supports the Municipality's Corporate Governance of ICT Policy.

31. SCOPE

The ICT User Access Management Policy has been developed to guide and assist municipalities to be aligned with internationally recognised best practice User Access Management controls and procedures. This policy further recognizes that municipalities are diverse and therefore adopts the approach of establishing principles and practices to support and sustain the effective control of user access management in the Municipality.

The policy applies to everyone in the municipality, including its service providers/vendors. This policy is regarded as being crucial to the operation and security of ICT systems of the Municipality. Municipalities must develop their own User Access Management controls and procedures by adopting the principles and practices put forward in this policy.

The policy covers the following elements of user access management:

- New user registration;
- Terminated user removal;
- User permission/role change request;

- User access rights assignment for networks, operating systems, databases and applications;
- Reviewing user access permissions; and
- User and administrator activity monitoring.

Aspects relating to ICT security and operating system security controls are contained in the ICT Security Controls and ICT Operating System Security Controls policies.

32. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the Municipality and evaluated on its level of severity. Appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy. Actions include, but are not limited to:

- Revocation of access to Municipal systems and ICT services;
- Disciplinary action in accordance with the Municipal policy;
- Civil or criminal penalties e.g. violations of the Copyright Act, Act No. 98 of 1978; or
- Punitive recourse against the service provider/vendor as stated in the service provider/vendor's SLA with the Municipality.

33. ADMINISTRATION OF POLICY

The ICT Manager or delegated authority within the municipality is responsible for maintaining this policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and recommended changes must be approved by Council

34. DELEGATION OF RESPONSIBILITY

In accordance with the ICT Governance Policy, it is the responsibility of the Municipal Manager to determine the delegation of authority, personnel responsibilities and accountability to Management with regards to the Corporate Governance of ICT.

35. NEW USER REGISTRATION

35.1 A formalised user registration process must be implemented and followed in order to assign access rights.

35.2 All user access requests must be formally documented, along with the access requirements, and approved by authorised personal by making use of the user access request form. The template for this type of request can be found attached to this policy in Annexure B.

35.3 User access requests must be obtained from HR on registration of a new employee. The form must be sent to the service provider/line manager for access requirements to be requested. Once the requirements have been requested and signed off by the departmental manager, the form must be sent to the ICT department for approval following which the activation of the employee based on the specified requirements will be completed. The form must then be sent back to HR for record keeping purposes. Records of user access granted must be stored for a minimum of 10 years.

35.4 User access must only be granted once approval has been obtained.

35.5 All users must be assigned unique user IDs in order to ensure accountability for actions performed. Should shared accounts be required to fulfil a business function, this account must be approved and documented by the Risk Management Committee.

35.6 The diagram below depicts the formal new user registration process to be followed.

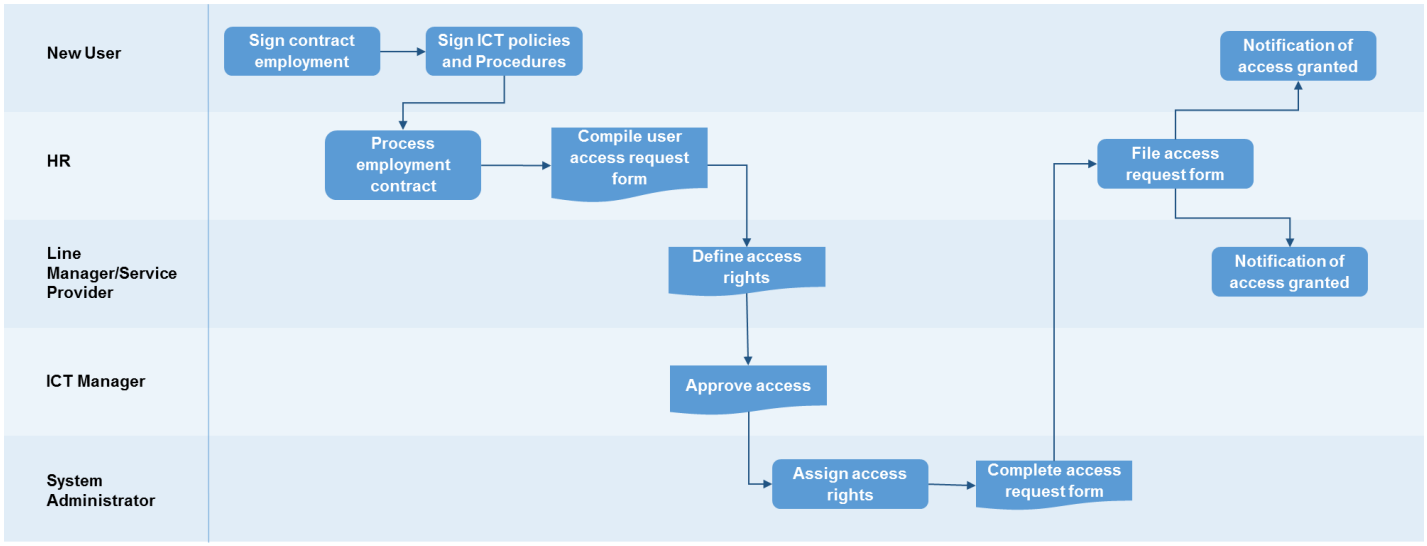


Figure 2: New user registration process

36. TERMINATED USER REMOVAL

36.1 A formalised user termination process must be implemented and followed in order to revoke access rights.

36.2 All user termination requests must be formally documented and approved by duly authorised personnel. Access must be disabled immediately, with accounts being removed after 6 months once authorisation has been obtained by line manager.

36.3 Terminated user requests must be obtained from HR on the termination of an employee. The template for this type of request can be found attached to this policy in Annexure B. The form must be sent to the service provider/line manager for access revocation to be signed off. Once access revocation has been signed off, the form must be sent to the ICT department for approval and deactivation of employee based on specified requirements. The form must then be sent back to HR for record keeping purposes. Records of user access removal must be stored for a minimum of 10 years.

36.4 The diagram below depicts the formal user termination process to be followed.

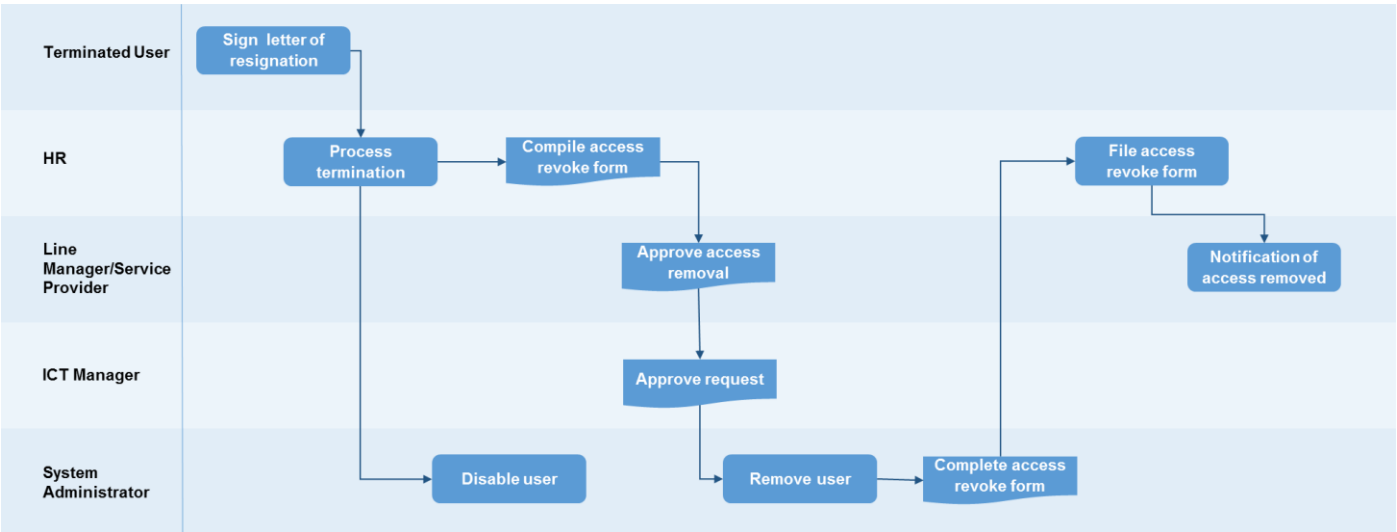


Figure 3: User termination process

37. USER PERMISSION/ROLE CHANGE REQUEST

37.1 A formalised user access management process must be implemented and followed in order to adjust user access rights.

37.2 All user access change requests must be formally documented, along with their access requirements, and approved by duly authorised personnel.

37.3 Access must only be granted once approval has been obtained by the respective line manager.

37.4 User access change requests must be obtained from HR on change of an employee's role or permissions. The template for this type of request can be found attached to this policy in Annexure B. The form must be sent to the service provider/line manager for access requirements to be signed off. Once the access requirements have been signed off, the form must then be sent to the ICT department for approval and adjustment of employee's access rights based on specified requirements. The form must then be sent back to HR for record keeping purposes. Records of user access granted and removed must be stored for a minimum of 10 years.

37.5 User access rights that are no longer required must be removed immediately.

37.6 The diagram below depicts the formal user permission/role change request process to be followed.

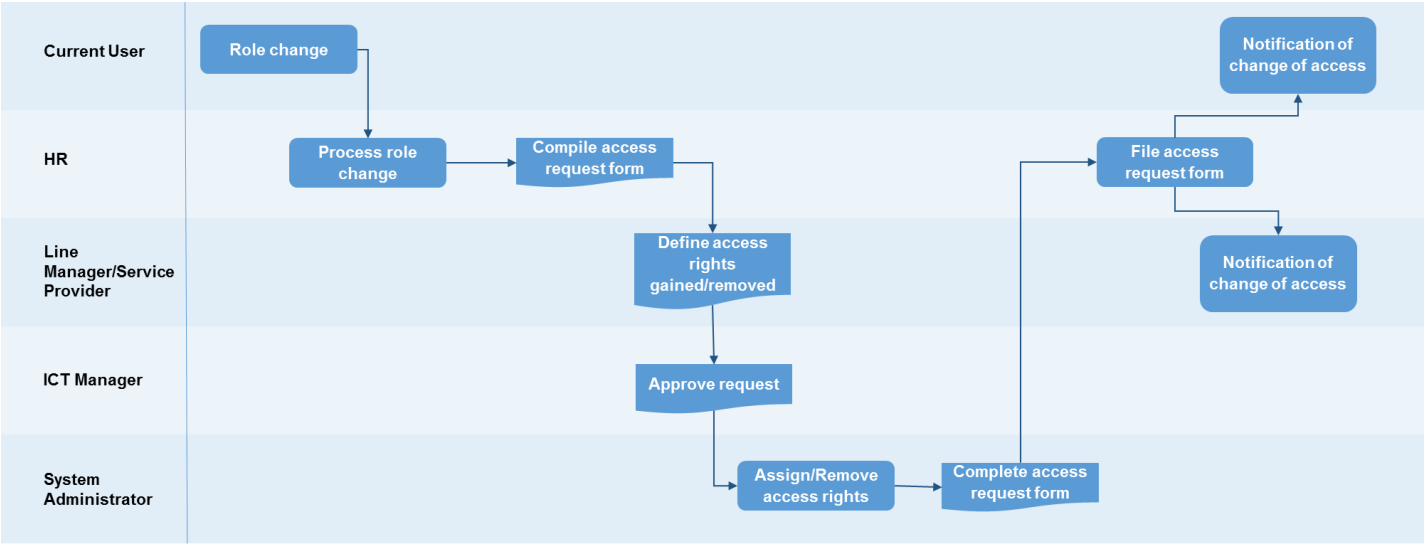


Figure 4: User permission/role change request process

38. GENERAL USER ACCESS RIGHTS ASSIGNMENT

38.1 Access rights include, but are not limited to:

(a) General office applications (E-mail, Microsoft Office, SharePoint, etc.);

(b) Department specific applications and/or databases;

(c) Network Shares;

(d) Administrative tasks;

(e) RAS/VPN Access;

(f) Wi-Fi; and

(g) BYOD.

38.2 Access must follow a "principle of least-privilege" approach, whereby all access is revoked by default and users are only allowed access based on their specific requirements.

38.3 The levels or degrees of access control to classified information must be restricted in terms of legislative prescripts.

38.4 Access rights must be assigned to a group/role. A user must then be assigned to that group. Access rights must not be assigned to individual users.

39. NETWORK USER ACCESS RIGHTS ASSIGNMENT

39.1 Access to the Municipality's network must only be allowed once a formal user registration process has been followed.

39.2 Access to Wi-Fi must only be provided to users who require access to the network throughout the Municipality, to fulfil their business function.

39.3 RAS/VPN access must only be granted to users who require the service to fulfil their business function.

39.4 Best practice states that RAS access must only be granted to employees who require remote access to a system in order to administer the environment.

39.5 Best practice states that VPN access must only be granted to employees who:

(a) Work remotely (Not at the office);

(b) Work overtime, or not within regular office hours.

39.6 It is the responsibility of the ICT Steering Committee to ensure all users must be made aware of the security risks and obligations associated with RAS/VPN access.

39.7 RAS/VPN access must be monitored and audit logs reviewed every quarter (3 months) by system administrators.

39.8 All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes. Records of RAS/VPN access reviews must be stored for a minimum of 10 years.

39.9 The ICT Manager must approve all hardware and software, owned by Municipal employees and service providers/vendors, if it is to be used for official purposes (BYOD).

39.10 The ICT team must ensure that all mobile devices must be protected with a PIN.

40. OPERATING SYSTEM ACCESS RIGHTS ASSIGNMENT

40.1 Each system administrator must be given their own accounts within the administrator group. Should shared accounts be required to fulfil a business function, then this account must be approved and documented by the Risk Management Committee.

40.2 The default administrator account must be renamed and a password must be randomly generated and sealed in an envelope and kept in a safe.

40.3 The default guest account must be removed or renamed and disabled.

41. APPLICATION USER ACCESS RIGHTS ASSIGNMENT

41.1 Segregation of duties must be practiced, in such a way that application administrators cannot perform general user tasks on an application. This is to prevent any fraudulent activity from taking place.

41.2 Applications administrators must remain independent of the department utilising the application, with the exception of the ICT department.

42. DATABASE USER ACCESS RIGHTS ASSIGNMENT

42.1 The ICT Manager must limit full access to databases (e.g. sysadmin server role, db_owner database role, sa built-in login etc.) to ICT staff who need this access. Municipal employees who use applications may not have these rights to the application's databases.

42.2 The ICT Manager must ensure that Municipal employees who access databases directly (e.g. through ODBC) only have read access.

42.3 The ICT Steering Committee must approve all instances where Municipal employees have edit or execute access to databases.

42.4 The ICT Manager must review database rights and permissions on a quarterly basis (every 3 months). Excessive rights and permissions must be removed.

43. REVIEWING USER ACCESS AND PERMISSIONS

43.1 User access and user permissions must be reviewed every quarter (3 months) by system administrators.

43.2 On a monthly basis, HR must send a list of all terminated employees for that month to the ICT department. This list must be used to ensure that all terminated users have had their access revoked. Should one or more terminated users still have access to the environment, and investigation into the finding must be conducted.

43.3 On a monthly basis, the ICT Manager must review all users with administrative access to the environment and assess their rights for appropriateness. Should a user be found with excessive rights, a user access change request must be performed.

43.4 All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes. Records of user access review must be stored for a minimum of 10 years.

44. USER AND ADMINISTRATOR ACTIVITY MONITORING

44.1 User and administrator activity must be monitored through audit and event logging.

44.2 Once a month, system administrators and application owners must review audit and event logs for suspicious and malicious activities. A template for the reviewing of audit logs can be found in Appendix D of this Policy.

44.3 Dormant accounts should be disabled and a request to remove the access should be performed in line with section 11. User Permission/Role Change Request.

44.4 All reviews must be formally documented and signed off by the ICT Manager. Documentation must be kept for record keeping purposes. Records of user activity monitoring must be stored for a minimum of 10 years.

45. ANNEXURE A: IMPLEMENTATION ROADMAP

No	Action	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	Identify all current access management procedures																		
2	Assess appropriateness of current procedures																		
3	Adjust and document changes to procedures																		
4	Educate employees of changes in procedures																		
5	Implement newly defined or adjusted procedures																		

46. ANNEXURE B: USER ACCESS MANAGEMENT FORM EXAMPLE

Name:
_____ Date: ___/____/____

Designation:

New Termination Change

Requested by: _____
_____
__

General PC Use
E-mail
VPN
RAS
Finance Application
HR Application
Comms Application
_____
(other)
_____
_____
_____

Administrative rights:

☐
☐
☐
☐
☐
☐

The following section must be completed if access is being requested for a service provider/vendor:

Period of access: _____

Reason for request:

Signatures:

HR Manager_____ Line Manager_____

Date: ___/____/____ ___/____/____

ICT Manager _____ System Administrator_____

Date: ___/____/____ _____/_____/_____

47. ANNEXURE C: OPERATING SYSTEM SECURITY SETTINGS

Security Configuration	Setting
Password Policy - General User Accounts	
Minimum password length	8 characters
Maximum password age	30 days
Password history	6passwords emembered
Password complexity	Enabled
Password Policy - Administrative/Super User Accounts	
Minimum password length	12 characters
Maximum password age	30 days
Password history	12 passwords remembered
Password complexity	Enabled
Account Lockout Policy - General User Accounts	
Account lockout duration	60 minutes
Account lockout threshold	3 attempts
Account lockout counter threshold	30 minutes
Account Lockout Policy - Administrative/Super User Accounts	
Account lockout duration	60 minutes
Account lockout threshold	3 attempts
Account lockout counter threshold	60 minutes
Audit Policy	
Account logon events	Failure
Account management	Success, Failure
Logon events	Failure
Policy change	Success, Failure
Privilege use	Success, Failure
System events	Failure

48. ANNEXURE D: AUDIT/EVENT LOG REVIEW TEMPLATE

Reviewer:			
Month/Year	____/20___		
System/Application	Day of review	Signature	Notes
Active Directory			
Exchange			
Member Server 1			
Member Server 2			
Member Server 3			
Member Server 4			
Finance Application			
HR Application			
Comms Application			
Document Management System			

ICT Manager Signature: _____

Date: ___/____/20__

49. ANNEXURE E: REFERENCES

BS ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls. (2013). Geneva: BSI Standards Limited.
Control Objectives for Information Technology (COBIT) 5. (2012). Illinois: ISACA.
Minumum Information Security Standards. (1996, December 4). Cabinet.

ICT SERVICE LEVEL AGREEMENT MANAGEMENT POLICY (ICT and Municipality)

TABLE OF CONTENTS

Glossary of Abbreviations

Abbreviation	Definition
COBIT	Control Objectives for Information and Related Technology
ICT	Information and Communication Technology
IDP	Integrated Development Plan
ISM	Information Security Manager
ISO	International Organization for Standardisation
SDBIP	Service Delivery and Budget Implementation Plan

Glossary of Terminologies

Terminology	Definition
Catalogue	A complete list of items.
Staff performance agreements	Includes, but not limited to, the performance agreements of the Municipal Manager or a manager directly accountable to the Municipal Manager. This includes performance objectives and targets that must be met, and the time frames within which those performance objectives and targets must be met. This also includes the consequences of substandard performance.

50. INTRODUCTION

The Municipality uses ICT services, applications and tools on a daily basis to achieve its strategic goals and objectives. It is therefore important for the ICT function to understand the Municipality's requirements in respect of ICT services in order to manage ICT services within the environment. This is referred to as Service Level Management between ICT and the Municipality.

51. LEGISLATIVE FRAMEWORK

The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

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

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996.
- 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.
- 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 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.
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls.
- King Code of Governance Principles, 2009.

52. OBJECTIVE OF THE POLICY

The objective of the policy is to align the ICT strategic goals and objectives with the Municipality's strategic goals and objectives. Additionally the policy creates visibility of ICT services being provided to the Municipality, thereby allowing for better and improved management of services.

53. AIMS OF THE POLICY

The aim of this policy is to provide a set of principles, practices and functions for service level management between ICT and the Municipality that is aligned to the Municipal ICT Governance Policy.

54. SCOPE

This ICT Service Level Agreement Policy has been developed to guide and assist municipalities to be aligned with internationally recognised best practice standards. This policy applies to the Municipal Manager and the ICT Manager involved in setting and managing service levels between ICT and the Municipality.

This policy is regarded as being crucial to the operation and security of ICT systems of the Municipality.

The policy covers the following elements of service level agreement management between ICT and the Municipality:

- Agreement between ICT and the Municipality; and
- Service management.

55. ADMINISTRATION OF POLICY

The ICT Manager or service provider/vendor is responsible for maintaining the policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and any changes approved by the Council.

56. AGREEMENT BETWEEN ICT AND THE MUNICIPALITY

56.1 The ICT Manager must create a catalogue of all ICT services and standardised applications and technologies required to deliver such ICT services. The register must include a description of the service, how it is delivered, the cost, the frequency, response time and minimum service levels.

56.2 The ICT Manager must review the ICT services with all directorates on an annual basis to ensure that the service still meets their requirements.

56.3 The ICT Manager must review the IDP and SDBIP with the all directorates on an annual basis to highlight opportunities to exploit ICT technology. During which, the

ICT Manager must update the catalogue of ICT services with the decisions made during these sessions.

56.4 The ICT Manager must establish baselines to measure performance of each ICT service.

57. SERVICE MANAGEMENT

57.1 The catalogue of ICT services must be translated into staff performance agreements.

57.2 The ICT Manager must collect data to determine if the ICT services are delivered successfully.

57.3 The ICT Manager must deliver a report on the ICT service levels to the ICT Steering Committee at every committee meeting.

57.4 Actions plans must be identified by the ICT Manager for performance issues and agreed with the ICT Steering Committee.

57.5 The ICT Steering Committee must monitor the resolution of the agreed actions.

57.6 The ICT Steering Committee may grant a reduction in response time and minimum service levels for ICT services if they are not feasible or cost effective.

58. ANNEXURE A: IMPLEMENTATION ROADMAP

No	Action	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6
1	Create a catalogue of ICT services						
2	Review the catalogue of ICT services with directorates						
3	Review the IDP and SDBIP to determine ICT opportunities						
4	Agree the ICT services catalogue with the Municipal manager						
5	Commence review of ICT service levels (Continuous)						

59. ANNEXURE B: EXAMPLE ICT SERVICES CATALOGUE

Service description	Access to the service	ICT internal cost (shared costs apportioned to more than one service)	Frequency	Response time	Minimum service level
User services					
Network access	Requests and failts logged at the ICT helpdesk	Network switches and routers (Rx) Cabling (Rx) Installation of network points (Rx) Wireless access points (Rx) Network monitoring software (Rx) ICT network technician (Rx) ICT outsource partner LAN support (Rx) Server hardware (Rx) Microsoft enterprise agreement (Rx) ICT helpdesk software (Rx) ICT Manager (Rx)	<u>On demand</u> Issue of network account Removal of network accounts Network password resets <u>Continous</u> Network connectivity	Request completed within 1 day Installation of network point within 5 days	Network access available 98% of the time, 24 hours a day, 7 days a week, except for scheduled maintenance windows

Service description	Access to the service	ICT internal cost (shared costs apportioned to more than one service)	Frequency	Response time	Minimum service level
Internet access	Requests and failts logged at the ICT helpdesk	Internet service provider (Rx) ICT network technician (Rx) ICT outsource partner WAN support (Rx) Firewall (Rx) Network switches and routers (Rx) Software to filter e-mail and Internet traffic (Rx) Server hardware (Rx) Intruder prevention software (Rx) ICT helpdesk software (Rx) ICT Manager (Rx)	On demand Issue of internet access Removal of internet access Continous Internet connectivity	Request completed within 1 day	Internet access avialable 90% of the time, 24 hours a day, 7 days a week, except for scheduled maintenance windows
Remote access to the network as if you were working in the office	Requests and failts logged at the ICT helpdesk	VPN software (Rx) Firewall (Rx) Servers (Rx) ICT outsource partner support (Rx) Internet service provider (Rx) Microsoft enterprise agreement (Rx) ICT helpdesk software (Rx) ICT Manager (Rx)	On demand Issue of remote access Removal of remote access Mobile device connectivity Continous Remote access service	Request completed within 1 day	Remote access available 95% of the time, 24 hours a day, 7 days a week, except for scheduled maintenance windows
E-mail and calendaring	Requests and failts logged at the ICT helpdesk	Firewall (Rx) Servers (Rx) Software to filter e-mail and Internet traffic (Rx) Domain name service (Rx) ICT network technician (Rx) ICT outsource partner LAN support (Rx) Internet service provider (Rx) Microsoft enterprise agreement (Rx) ICT helpdesk software (Rx) Backup and disaster recovery (Rx) ICT Manager (Rx)	On demand Issue of mailbox Removal of mailbox Continous E-mail service	Request completed within 1 day	E-mail available 98% of the time, 24 hours a day, 7 days a week, except for scheduled maintenance windows

Service description	Access to the service	ICT internal cost (shared costs apportioned to more than one service)	Frequency	Response time	Minimum service level
File server	Requests and failts logged at the ICT helpdesk	Servers (Rx) ICT network technician (Rx) Microsoft enterprise agreement (Rx) ICT outsource partner LAN support (Rx) ICT helpdesk software (Rx) Backup and disaster recovery (Rx) ICT Manager (Rx)	<u>On demand</u> Granting of file server access Removal of file server access Maintenance of directory access <u>Continous</u> File server access	Request completed within 1 day	File server available 98% of the time, 24 hours a day, 7 days a week, except for scheduled maintenance windows Allocation of xGB disk space for each user
Printing and faxing	Requests and failts logged at the ICT helpdesk	Servers (Rx) ICT network technician (Rx) Printer hardware supply and maintenace contract (Rx) Fax service (Rx) ICT helpdesk software (Rx) ICT Manager (Rx)	<u>On demand</u> Printer installation Printer setup Removal of printer Fax setup <u>Continous</u> Print services	Request completed within 5 days	Network print services available 95% of the time, 24 hours a day, 7 days a week, except for scheduled maintenance windows
Desktop & laptop installation, moves and changes	Requests and failts logged at the ICT helpdesk	Desktop & laptop supply and repair contract (Rx) ICT desktop support technician (Rx) Desktop & laptop software (Rx) Microsoft enterprise agreement (Rx) Anti-virus software and maintenance (Rx) Software license management (Rx) Insurance (Rx) Software patch management (Rx) ICT helpdesk software (Rx) Data backup (Rx) ICT Manager (Rx)	<u>On demand</u> Desktop and laptop hardware installation, moves and changes Software installation, moves and changes Cleaning of viruses Data recovery Encryption of devices <u>Continous</u> Software upgrades Anti-virus services Inventory management	Request completed within 3 days, unless third level support required	-

Service description	Access to the service	ICT internal cost (shared costs apportioned to more than one service)	Frequency	Response time	Minimum service level
Telephony and audio visual	Requests and failts logged at the ICT helpdesk	Switchboard and telephony devices (Rx) VOIP software (Rx) ICT outsource partner LAN support (Rx) ICT network support technician (Rx) Cabling (Rx) Video conferencing equipment (Rx) Inventory management (Rx) Servers (Rx) ICT helpdesk software (Rx) ICT Manager (Rx)	On demand Telephone device installation, moves and changes Voicemail activitation Video conferencing support Continous Telephony services Inventory management	Request completed within 1 day, unless third level support required Video conferencing requests completed within 2 hours	Telephony services available 98% of the time, 24 hours a day, 7 days a week, except for scheduled maintenance windows
Training	Requests logged at the ICT helpdesk	ICT training service provider (Rx) eLearning software and hardware (Rx) ICT Manager (Rx)	On demand User training Continous eLearning solution	Request completed within 60 days	-
Municipal systems					
Financial system	ICT change request	ICT developer (Rx) Software maintenace contract (Rx) Server hardware and software (Rx) Storage hardware (Rx) Database support (Rx) ICT database administrator (Rx) Server room costs (Rx) Backup and disaster recovery (Rx) Data capture staff (Rx) ICT Manager (Rx)	On demand Application maintenance and support Continous Application availability	Financial system available 95% of the time, 24 hours a day, 7 days a week, except for scheduled maintenance windows	Request generally completed within 5 days, except for complex requests
Human Resources system	ICT change request	Software maintenance contract (Rx) Server hardware and software (Rx) Storage hardware (Rx) Server room costs (Rx) Backup and disaster recovery (Rx) Data capture staff (Rx) ICT Manager (Rx)	On demand Application maintenance and support Continous Application availability	Financial system available 97% of the time, 24 hours a day, 7 days a week, except for scheduled maintenance windows	Request generally completed within 5 days, except for complex requests

Service description	Access to the service	ICT internal cost (shared costs apportioned to more than one service)	Frequency	Response time	Minimum service level
Other system	ICT change request	ICT outsource partner project cost (Rx) Business analyst (Rx) Software procurement (Rx) Server hardware (Rx) Middelware software (Rx) Storage hardware (Rx) Web hosting service (Rx) Server room costs (Rx) Extra network bandwidth (Rx) Backup and disaster recovery (Rx) Data capture staff (Rx) ICT Manager (Rx)	<u>On demand</u> Application maintenance and support <u>Continous</u> Application availability	Financial system available 90% of the time, 24 hours a day, 7 days a week, except for scheduled maintenance windows	Request generally completed within 20 days, except for complex requests
Access to municipal systems	Requests logged at the ICT helpdesk	ICT developer (Rx) ICT database administrator (Rx) ICT network support technician (Rx) Microsoft enterprise agreement (Rx) ICT Software maintenace contract (Rx) ICT helpdesk software (Rx) ICT Manager (Rx)	<u>On demand</u> Granting, ammendment and removal of access Password resets <u>Continous</u> User access facilities	Request completed within 2 days	-

60. ANNEXURE B: REFERENCES

BS ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls. (2013). Geneva: BSI Standards Limited.
Control Objectives for Information Technology (COBIT) 5. (2012). Illinois: ISACA.
King Code of Governance for South Africa. (2009). Institute of Directors in Southern Africa.
Local Government: Municipal Finance Management Act, No. 53. (2003). Republic Of South Africa.
Local Government: Municipal Structures Act 117. (1998). Republic of South Africa.
Local Government: Municipal Systems Act 32. (2000). Republic of South Africa.

ICT SERVICE LEVEL AGREEMENT MANAGEMENT POLICY (EXTERNAL SERVICE PROVIDERS/VENDORS)

TABLE OF CONTENTS

Glossary of Abbreviations

Abbreviation	Definition
COBIT	Control Objectives for Information and Related Technology
ICT	Information and Communication Technology
ISM	Information Security Manager
ISO	International Organization for Standardisation

Glossary of Terminologies

Terminology	Definition
Clauses	Contract terms and conditions.
Contract meetings	A scheduled meeting with a service provider/vendor with supporting evidence.
Cost structure	The methodology to calculate a service fee. It may include, but are not limited to, a fixed fee component, fee per deliverable, fee per usage of a product, etc.
Deliverables	The outcomes expected from a service provider. It may include, but are not limited to, documents, knowledge transfer, installed software, a service, etc.
Escalate	To formally inform another party in writing or through electronic communications asking for a course of action.
Intellectual property rights	Any copyrighted materials, patents, trademarks, industrial designs and geographical indications and names of origin registered by a third party. Also includes commercial secrets governed under a confidentiality agreement.
Performance reviews	Comparing expected and agreed performance against actual performance based on measurable outcomes.
Sub-contractors	A primary contractor entering into agreements with other entities to deliver the service of the primary contractor.

61. INTRODUCTION

The delivery of ICT services to the Municipality requires specialist skills and varying capacity demands. The use of external service providers/vendors to provide ICT services can be a cost effective and reliable way of acquiring these skills at a reasonable cost and in the required timeframes. As a result, information security risks also extend across the supply chain and therefore service providers/vendors of ICT related services must be managed to ensure that these risks are controlled and mitigated where possible.

ICT remains accountable for ICT services under the control of service providers/vendors. It is for this reason that the management of service providers/vendors is an important Municipal task to ensure that service providers/vendors deliver the agreed services within the agreed timeframes and cost.

62. LEGISLATIVE FRAMEWORK

The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

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

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996.
- 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.
- 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 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.

- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls.
- King Code of Governance Principles, 2009.

63. OBJECTIVE OF THE POLICY

The objective of the policy is to ensure that ICT-related resource needs are met in an efficient and structured manner.

64. AIMS OF THE POLICY

The aim of this policy is to provide a set of principles, practices and functions for ICT service provider/vendor/vendor management that are aligned to national and international best practice frameworks. It is a requirement of the Municipal ICT Governance Policy to implement service provider/vendor management as an integral part of corporate governance within the Municipality.

65. SCOPE

This policy recognizes that municipalities are diverse in nature, and therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of service level agreement management. The policy covers the supply of ICT hardware, software, services and personnel.

This policy is regarded as crucial to the operation and security of ICT systems of the Municipality.

The policy covers the following elements of service level agreement management of external service providers/vendors:

- Agreement with service providers/vendors/vendors;
- Service management; and
- Change control.

66. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the Municipality and evaluated on its level of severity. Appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy. Actions include, but are not limited to:

- Revocation of access to Municipal systems and ICT services;
- Disciplinary action in accordance with the Municipal policy; or
- Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978).

- Recourse against the service provider in terms of the contract terms.

67. ADMINISTRATION OF POLICY

The ICT Manager or service provider/vendor is responsible for maintaining the policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and any changes approved by the Council.

68. AGREEMENTS WITH SERVICE PROVIDERS/VENDORS

68.1 Over and above the default government terms and conditions, the following terms and conditions must be defined in all ICT service provider/vendor contracts:

(a) A description of the ICT services and how they will be delivered;

(b) The monthly fees and deliverables attached to the fees;

(c) The cost structure and payment schedule;

(d) The period of the contract, renewal and termination clauses;

(e) Availability, reliability and capacity of person/s responsible for delivering the service;

(f) Confidentiality and non-disclosure;

(g) In the case of software development:

- Who owns the program as well as the ideas and processes that makes it a valuable piece of software within the Municipal environment;
- Who is responsible for testing and ensuring that users are completely satisfied, as well as who is responsible for ensuring that users are able to use the software successfully;
- Who is responsible for, and how, the software will be maintained in the future;

(h) Which data the service provider/vendor may have access to, who owns the data, and how the data must be protected in line with the ICT Security Controls Policy;

(i) The responsibilities of both parties for ICT disaster recovery;

(j) Municipality's involvement in service provider/vendor processes, as well as the right to send its own audit team;

(k) Service Provider/Vendor service reporting;

(l) How the service provider/vendor will ensure that the resources/skills are available for the duration of the agreement;

(m) Skills transfer to the Municipality;

(n) Monitoring of critical systems in real-time and providing appropriate alerts to the ICT Manager.

(o) The security requirements of the person(s) delivering the ICT service in line with the ICT Security Controls Policy as well as the ICT Operating System Security Controls Policy;

(p) Should the service provider/vendor store or process personal information on behalf of the Municipality, the contract must state that the information must be protected in line with the ICT Security Controls Policy.

(q) Restrictions on the use of sub-contractors;

(r) In the event of a security breach affecting personal information, the service provider/vendor must notify the Municipality immediately;

(s) Penalties or discounts for non-performance against service levels;

(t) The process to terminate the agreement, without disrupting the ICT service to the Municipality; and

(u) Monthly status meeting.

68.2 The ICT Manager must ensure that service providers/vendors produce reports that include, but not limited to, the following information:

- Service level performance statistics, with failures and consequences;
- Major events;
- Incidents logged and resolution;
- Capacity usage and growth trends;
- Change requests and status; and
- Details of charges and invoices.

68.3 The agreement with the service provider/vendor must indicate the response time from the service provider/vendor based on the level of impact. The table below contains an example:

Impact	Description	Service level
Priority 1	The whole Municipality affected Extensive financial impact	2 hours
Priority 2	More than half of Municipality affected Single department affected Significant financial impact	4 hours
Priority 3	Single user affected by an incident Limited financial impact	24 hours
Priority 4	Enhancement or new capability Service request from a user	To agreed timelines

Table 6 : Example service level determined by impact

68.4 All ICT contracts must be stored centrally in the Municipal archive. Ideally contracts must also be stored in electronic form in a contract management system where they are easily accessible to those managing the service.

69. SERVICE MANAGEMENT

69.1 The ICT Steering Committee must nominate the ICT Manager as the service manager for each ICT contract. The ICT Steering Committee may nominate any other Municipal employee to manage the service of ICT-related contracts if the contract is outside of the ICT Manager's scope of responsibility e.g. a financial or human resources system.

69.2 The ICT Manager must ensure that the services received from service providers/vendors are dependent on contact meetings and performance reviews. The amount of time and effort spent managing service providers/vendors must be equal to their importance to the Municipality.

69.3 The following table is a broad guideline of the categories of service providers/vendors and the level of service management required by this policy:

Categories of service providers/vendors	Description	Example
Strategic	This is a significant agreement that involves a lot of participation by the ICT Manager. This agreement is often long term and involves sharing of Municipal data. This agreement would require monthly contact and service reviews. The contract and SLAs must be reviewed twice a year.	ICT outsourcing Supply of network services
Tactical	This is a significant agreement that would normally be managed by the ICT Manager. This agreement would require monthly contact and service reviews. The contract and SLAs must be reviewed twice a year.	Hardware maintenance and repair End-user support services
Operational	This type of agreement is for the supply of operational products and services and would normally be managed by the ICT Manager. This agreement would require quarterly contact and service reviews. The contract and SLAs must be reviewed once a year.	Internet hosting service provider
Commodity	This type of agreement is for the supply of low-value and readily available products and services. The agreement is normally managed by ICT staff and the normal supply chain management controls would suffice.	Personal computers Printer consumables

Table 7 : Categories of service providers

69.4 The ICT Manager is responsible to review the ability of the service provider/vendor to continue delivering the service in the near future as well as dealing with contract disputes and renewals.

69.5 The ICT Manager must inform the ICT Steering Committee on a monthly basis of known service delivery failures on Strategic and Tactical contracts. The ICT Manager must escalate continued service delivery failures to the ICT Steering Committee at their next scheduled meeting.

69.6 The ICT Manager must deal with known service delivery failures on Operational contracts on a quarterly basis.

69.7 The ICT Manager must communicate unsatisfactory performance by service providers/vendors in writing compelling the service provider/vendor to perform according to the contract.

69.8 If any dispute arises, the process is to first attempt to reach an amicable agreement. Secondly, the parties can go for mediation. Thirdly, the matter may be settled in a South African court of law.

69.9 Termination of the contract must be considered, as stipulated in the general conditions of contract, for reasons such as delayed deliveries, failing to perform any other contractual obligation or if the service provider/vendor has engaged in corrupt and fraudulent practises and insolvency.

69.10 Contract termination may be effected if allowed for in the contractual conditions and if both parties agree to the termination in writing.

69.11 The ICT Steering Committee may enforce discounts or penalties from service providers/vendors if the contract conditions provide for this.

69.12 The ICT Manager is responsible to ensure that ICT service provider/ vendor environments are audited.

70. CHANGE CONTROL

70.1 The ICT Manager must ensure that agreements are kept up to date with changes to the ICT service.

70.2 The ICT Manager must ensure that the introduction of a new service provider/vendor and a major change to an existing agreement must be controlled through the change control process defined in the ICT Security Controls Policy.

70.3 The ICT Manager must ensure that service providers/vendors follow the change control process defined in the ICT Security Controls Policy for changes to the ICT environment.

71. ANNEXURE A: IMPLEMENTATION ROADMAP

No	Action	Month 1	Month 2	Month 3	Month
1	Identify all ICT contracts				
2	Allocate ICT Contract Managers to all ICT contracts				
3	Identify ICT service providers/vendors that process personal information				
4	Review all ICT contracts against prescribed minimum terms				
5	Commence management of ICT contracts (Continuous)				

72. ANNEXURE B: REFERENCES

BS ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls. (2013). Geneva: BSI Standards Limited.
Control Objectives for Information Technology (COBIT) 5. (2012). Illinois: ISACA.
King Code of Governance for South Africa. (2009). Institute of Directors in Southern Africa.
Local Government: Municipal Finance Management Act, No. 53. (2003). Republic Of South Africa.
Local Government: Municipal Structures Act 117. (1998). Republic of South Africa.
Local Government: Municipal Systems Act 32. (2000). Republic of South Africa.
Protection of Personal Information Act, No. 4. (2009). Republic of South Africa.

ICT DISASTER RECOVERY POLICY

TABLE OF CONTENTS

Glossary of Abbreviations

Abbreviation	Definition
BCMS	Business Continuity Management System
BC	Business Continuity
DR	Disaster Recovery
DRP	Disaster Recovery Plan
HR	Human Resources
ICT	Information and Communication Technology
MTO	Maximum Tolerable Outage
RTO	Recovery Time Objective
RPO	Recovery Point Objective
ITIL	Information Technology Infrastructure Library
RACI	Responsible, Accountable, Consulted, Informed
IROC	ICT Recovery Operations Centre
BAU	Business As Usual

Glossary of Terminologies

Terminology	Definition
Business case	A formal requirement in order for a specific business function to perform its required task, such as to implement a project initiative.
Line manager	Each department (HR, Finance, ICT, etc.) should have a manager employed to perform managerial tasks.
Main Site	Municipal Head Office and assumed in some case to be the location of the Municipality Main Data Centre
Maximum Tolerable Outage	The amount of time the identified critical business function may be unavailable before the Municipality is severely impacted.
ICT Recovery Operations Centre	The offsite command centre that gets established, by approval within the framework of the ICT DRP, for the purpose of ICT recovery operations & necessary relocation of identified resources.
Simulation Lite	A simulation DR test conducted by 2-3 individuals, usually the ICT Manager, the ICT DR Team Leader and an assistant.
Procurement	The external acquisition of services, assets and consumables, whether by outright purchase, hire, licensing or outsourcing.
Recovery Point Objective	The worst data loss that the Municipality is willing to accept. In other words, this is the point from which recovery of lost data must take place.

Terminology	Definition
Service	A Service delivered to the municipality by ICT or by 3rd parties. Examples: email, Internet, printing.
Contract	An agreement (which may be verbal or in writing) entered into with the intention of creating legally binding consequences. The contract includes all annexures, schedules, etc., as well as any agreed amendments.
Incident	Typically impacts a specific service or server. Examples of Incidents include a compromised service resulting from a hacking attack or the partial loss of an office area due to a burst water pipe.
Disaster	A significant or unusual Incident that has long-term implications. An example of a Disaster would be the loss of a building due to a fire.
Fit-for-purpose	An approach or solution that is pragmatic, by tailoring the scope of a piece of work, effort or solution to the prioritised elements, which can be better understood and operated.

Disaster (formal definition as per The Disaster Management Act)	The Disaster Management Act (Act No. 57 of 2002) defines a Disaster as a progressive or sudden, widespread or localised, natural or human-caused occurrence which:
	• Causes or threatens to cause:
	  ○ Death, injury and/or disease.
	  ○ Damage to property, infrastructure and/or the environment.
	  ○ Disruption of life, within the community.
	• Is of a magnitude that exceeds the ability of those affected by the Disaster to cope with its effects using only their own resources.

Test Guide	The DR Test Guide document provides guidance on the types, details, scheduling, effort and activity required for regular testing every year.
Power Cutback	An intentional situation in which the voltage in a power grid is reduced below its normal level, typically between 10-20% lower, to prevent complete power failure at the national grid.
Power Spike	Voltage spikes that occur for such a short duration of time, that may cause great damage to sensitive ICT equipment, by weakening semiconductor devices and frequently corrupting data in digital equipment.
Parallel ICT DR Test	In this test, the ICT DR Team simulate an actual ICT Disaster, by taking all relevant ICT DR Plan procedures, leaving the office, to an off-site venue or IROC, and activate VPN. The primary site is uninterrupted and critical systems are run in parallel at the alternative and primary sites.

Terminology	Definition
Full Interruption ICT DR Test	This test involves all aspects of the company in response to a Disaster. All steps in the plans are performed. Systems are shut down at the primary site and all individuals who would be involved in a real emergency, including internal and if possible, external organisations, participate in the test.

Incident versus Disaster

Business functions are vulnerable to a variety of disruptions, ranging from mild (e.g. short-term power outage, hardware failure, denial of access to the building, partial damage to offices) to severe (e.g. equipment destruction, fire). Vulnerabilities may be minimised or eliminated through technical, management, or operational solutions as part of the entities risk management effort.

However, it is virtually impossible to completely eliminate all risks. Contingency planning is designed to mitigate the risk of system and service disruption by focusing on effective and efficient recovery solutions.

In the context of this document and the documents listed in the Scope section, an Incident is distinguished from a Disaster.

The table below lists examples to help differentiate between Incidents and Disasters to assist in determining when the plan should be activated and when normal recovery will suffice.

Scenario	Possible causes	Impact	Recovery strategy
Destructive loss of building. *	Fire, explosion/ bomb, sabotage, flood, structural failure and natural Disasters.	• Almost all hardware, office infrastructure, equipment and non-electronic files are destroyed; and • Interruption of all business activities.	Activate the BCP /ICT DRP.
Loss of infrastructure.	Loss of power, flood, lightning, theft.	• Major loss of ICT Services; and • Core infrastructure is impacted and non-functional.	Activate ICT DRP.
Partial loss of building. *	Localised fire, explosion, bomb, sabotage, flooding, and power surge.	• Destruction of facilities and equipment in the affected area; • Possible damage to some areas of the building; and • Interruption of some business activities	Depending on damage assessment report activate BCP/DRP as necessary
Denial of access to building.	Public disturbances, civil unrest, closure by authorities, bomb threat.	• Staff cannot gain access to the building; • Limited, if any, impact on infrastructure; • Possible disruption of business activities; and • Critical systems can still be accessed remotely.	• Access systems remotely; and • Perform business activities remotely for a limited time.

73. INTRODUCTION

This policy guides the Municipality in the establishment, operation and continuous improvement of an ICT DR Framework: a system of five inter-dependant documents that co-exist to support the most important document i.e. the ICT DR Plan.

This policy provides background information on what ICT Disaster recovery is, as well as the role of this ICT policy, to provide governance and controls to manage the ICT Recovery capability of the Municipality.

The policy supports the Municipality's ICT Governance Policy and was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

73.1 ICT DR Framework

This ICT DR framework consists of five key documents, and resides in a broader landscape of relevant process within the Municipality. The five main ICT DR documents are listed as follows:

Document	Summary
ICT DR Policy.	• Broad policy, principles, high level framework & obligations.
ICT Risk & Impact Analysis.	• Risk & Vulnerability Analysis; and • Business Impact Assessment.
ICT DR Plan.	• Actionable Plan in event of Disaster incl. teams, processes & forms/templates.
ICT DR Architecture.	• Technical Assessments; • Architecture(s) for Current Live & DR environment; and • Service details.
ICT DR Test Guide	• Tiered Test plan.

Table 8: ICT DR Framework documents

Some key relationships may apply, to other important ICT documents and processes as listed below, but are not limited to that which is shown below:

- Backup and Recovery Policy;
- Incident Management process;
- Change Management process;
- Availability Management; and
- Service Level Agreement Management Policy.

74. LEGISLATION

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:

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
- 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;
- Promotion of Access to Information Act, Act No. 2 of 2000;
- Protection of Personal Information Act, Act No. 4 of 2013;
- The Disaster Management Act, Act No. 57 of 2002; Regulation of Interception of Communications Act, Act No. 70 of 2002; and
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

The following internationally recognised ICT 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;
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls; and
- King Code of Governance Principles, 2009.

75. OBJECTIVE OF THE POLICY

The objective of this document is to guide Municipal management to define the ICT DR policy so that an effective sustainable ICT DR Plan can be constructed, to enable the Municipality to enact an orderly and timely recovery from a Disaster or disruptive incident.

The controls within this policy seek to achieve the following objectives:

- Provide guidance on developing all related ICT DR documents, and prioritise the reason for the inter-relationships;
- Protect the operations of the Municipality, consumers, licensees, stakeholders and staff by minimising the impact of significant interruption to the Municipality through the effective implementation and maintenance of ICT DR arrangements and solutions;

- Recover the critical prioritised operations and services, in a controlled manner to meet the requirements of the department, law, regulation or other factors; and

- Ensure that business continuity is an essential part of business planning and future development, and that this policy be integrated into an overall municipal Disaster Management Plan at a later stage of business continuity being improved.

76. THE AIM OF THIS POLICY

The aim of this policy is to ensure that the Municipality conforms to standardised ICT Disaster recovery governance and controls, in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that the risks associated to the management of effective ICT DR, are mitigated.

This policy supports the Municipality's Corporate Governance of ICT Policy.

77. APPLICATION & SCOPE OF POLICY

The ICT DR policy will become a part of business continuity frameworks (such as BCMS – see Legislation Section) but focuses on a “fit for purpose” ICT DR approach that guides the authorised personnel, to recover internal and external ICT systems in the event of a Disaster.

This ICT DR Policy has been developed to guide and assist municipalities to be aligned with internationally recognised best practice DR controls and procedures. This policy further recognizes that municipalities are diverse and therefore adopts the approach of establishing principles and practices to support and sustain the effective control of Disaster recovery in the Municipality.

The policy applies to everyone in the municipality, including its service providers/vendors. This policy is regarded as being crucial to the operation and availability of ICT systems of the Municipality. Municipalities must customise their own ICT Disaster recovery controls and procedures by adopting the principles and practices put forward in this policy.

To give full effect to the DR planning and preparation in the Municipality, the broader group of ICT DR Documents are included in the planning process (see Section 1.1).
This DR policy and its inter-related documents gives full effect to the management of Disaster recovery in the Municipality, as demonstrated in the high level landscape of inter-related documents.

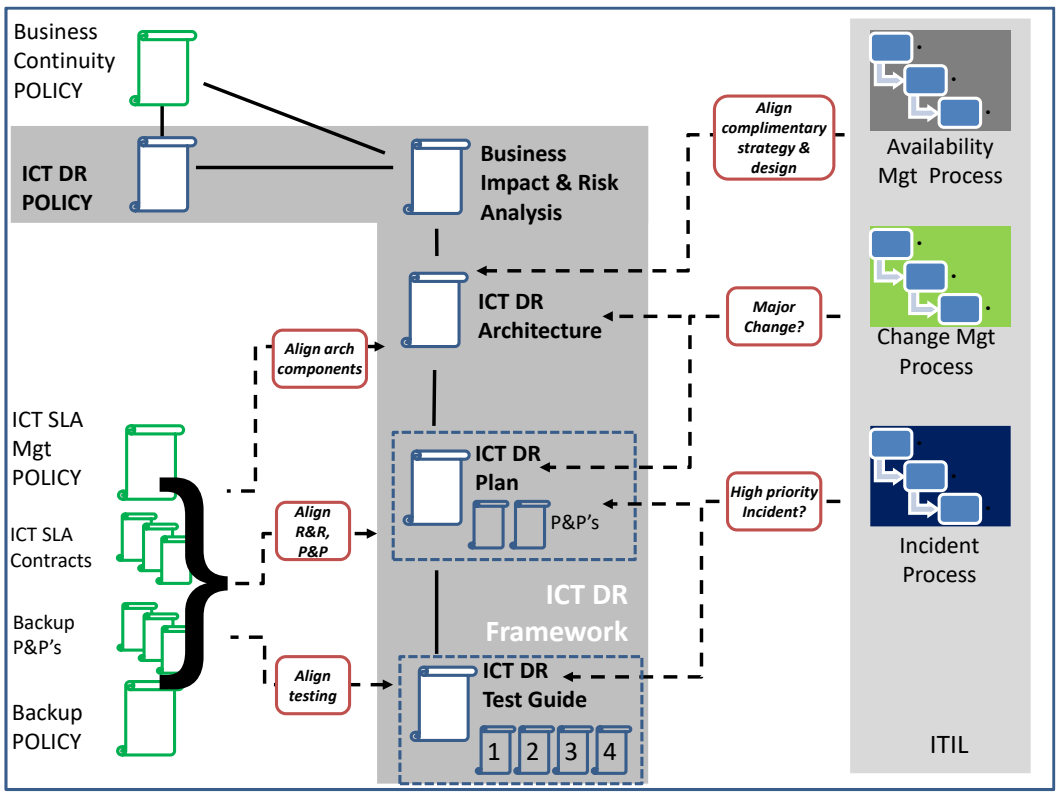


Figure 5: ICT DR Framework high level landscape

Note: Key dependencies will need to be managed continuously, specifically to the identification of critical services (in the event of critical service failures), supplied by external service providers, as governed and directed by the Service Agreement Policy.

This DR policy and its inter-related documents gives full effect to the management of Disaster recovery in the Municipality, as demonstrated in the high level landscape of inter-related documents (for more detail, refer to the ICT DR Architecture and the ICT DR Plan).

78. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the Municipality and evaluated on its level of severity. Appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy.

Actions include, but are not limited to:

- Revocation of access to Municipal systems and ICT services;
- Disciplinary action in accordance with the Municipal policy;
- Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978); or
- Punitive recourse against a service provider in terms of the contract.

79. CONFIDENTIALITY AND NON-DISCLOSURE

This document is confidential and must be treated as such. Distribution and usage of this document is subject to the signed confidentiality clause stipulated in employee contracts.

80. ADMINISTRATION OF POLICY

The ICT Manager or delegated authority within the municipality is responsible for maintaining this policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and recommended changes must be approved by Council.

81. DELEGATION OF RESPONSIBILITY

In accordance with the ICT Governance Policy, it is the responsibility of the Municipal Manager to determine the delegation of authority, personal responsibilities and accountability to the Management with regards to the Corporate Governance of ICT.

82. EXCEPTIONS

82.1 This policy does not include the Business Continuity Plan or the Business Continuity Management System, which are typically created in larger or mature municipalities, who have the resources, management and intent to drive such comprehensive frameworks.

82.2 This policy does not apply to broader BC-type components for business processes such as emergency response, financial, HR, Media, logistics and Marketing.

83. GENERAL POLICY

83.1 An ICT DR Team Leader must be appointed, along with an Alternate Leader.

83.2 A provisional ICT DR Team must be defined according to the roles and responsibilities of the ICT DR Plan.

83.3 A high level plan must be reviewed, by delegating specific documents, sections and activities to the ICT DR Team.

83.4 The ICT DR Plan is a critical document to be utilised by the municipality in the event of a Disaster. The ICT DR Plan helps guide recovery processes to the return of normal operations (termed as “Business As Usual” or BAU).

83.5 Any decision to implement an offsite Recovery Data Centre must consider a minimum radial distance of 6 km from the main Data Centre.

84. POLICY: External Policies and Processes

84.1.1 This policy will also make reference to other documents that will have inter-dependency, in the life-cycle of the ICT DR documentation.

84.1.2 These inter-dependencies must be explicitly documented, be updated regularly, and Municipal Committee informed via reporting of key status and changes.

84.1.3 These other policy and processes include, (but are not limited to):

- Business Continuity Policy (part of a BCMS);
- Incident Management Policy and process;
- Change Management Policy and process;
- Availability Management Policy; and
- SLA Management policy.

85. POLICY: ICT Business Impact and Risk Analysis

85.1 A formal impact and risk assessment shall be undertaken by/with Line Managers to determine the requirements for the Disaster recovery plan, from Municipal operations.

85.2 The ICT Manager must attend a minimum of 50% of all impact and risk analysis assessment meetings, with Line and/or Department Managers.

85.3 The ICT Manager must advise on the process and answer any key discrepancies in the development of the Impact and Risk analysis.

85.4 The individuals performing the business impact & risk analysis, must summarise the ICT system recovery requirements, to be communicated to the ICT Manager and the ICT team (including the MTO, RTO and RPO requirements.

85.5 The recovery requirements should categorise the Municipal operations or systems in levels of priority.

85.6 The ICT Manager and Line Managers, in consultation with the Municipal Manager, agree a document on key strategic decisions for ICT Recovery, for both onsite and offsite operations.

85.7 The Business Impact and Risk Analysis must be reviewed:

- Once a year; or
- Whenever there is a key identification that additional planning is required to cater for improved Disaster recovery to support the business.

85.8 The Municipality must prioritise an adequate and specific ICT DR strategy, and implementation of ICT availability controls, to cater for the significant risk of power grid failure in South Africa. The impact of loss of power (See Section 8.3: Loss of key dependencies, "ICT Business Impact and Risk Analysis") could be a realistic time period between a few hours and 2-3 weeks. The Municipality, as matter of policy, must implement:

- A suitable power generator to support a minimum of critical ICT servers, databases and prioritised operations.
- Adequate storage of diesel in close proximity to the power generators as a contingency to prevent catastrophic loss of ICT services in the event of a power failure.
- Evaluation of the probability of damage due to 'power cutbacks', and 'power spikes', that may impact critical equipment in the Data Centre and patch panels.
- Using this evaluation, the Municipality must justify the implementation of additional power line filtering, voltage clamping and UPS equipment (for very sensitive equipment and/or critical applications) to reduce the degree of impact.
- Physical testing of all power generators, diesel levels and UPS systems must occur at least every 3 months, in addition to scheduled ICT DR annual tests. These power tests must be prescribed by the ICT Manager in the ICT DR Test Guide document. The "Parallel" and "Full Interruption" ICT DR tests must specify whether or not a generator and UPS should be included in such tests.
- All technical details pertaining to power availability and DR strategy, such as: diesel generators, diesel tanks, UPS, wiring diagrams, and configuration summary, must be included in the ICT Disaster Recovery Architecture document.

86. POLICY: ICT DR Plan

86.1 The Municipality shall develop a comprehensive ICT Disaster recovery plan.

86.2 The ICT DR Plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.

86.3 All staff must be made aware of the ICT DR Plan and their own respective roles.

86.4 The ICT DR Plan is to be kept up to date every 3 months, to take into account changing circumstances.

86.5 A single ICT DR Team is to be appointed, with key roles and responsibilities, to own the process of recovery in the event of Disaster. Note that these roles will require various senior managers and representatives of the Municipality

86.6 The DR Plan must contain all relevant information, templates and procedures in order for the ICT DR Team to be informed (prior to, and during a Disaster) on how to recover the key ICT systems and applications.

87. POLICY: ICT DR Architecture

87.1 The ICT Manager must delegate, and co-ordinate a team of senior technical administrators to document the ICT technical architecture and its components.

87.2 The document must represent the:

- Current live ICT environment; and
- Current ICT Disaster Recovery architecture with attention to components.

87.3 All sections of this document must be updated:

- Every 6 months;
- Every time a configuration change impacts the ICT architecture;
- Every major Change Management activity that impacts architecture directly or indirectly;
- With sufficient detail on future necessary improvements depicted with the necessary schema, tables, gap analysis, functional notes and key DR functionality proposed changes; and
- With an updated relevant DR Roadmap that illustrates the active and proposed project activities, with relevance to DR capability and improvement.

88. POLICY: ICT DR Test Plan

88.1 All senior members of the Municipal Management, key stakeholders and service providers, must be informed of the annual DR Test Plan within 1 month of the start of the new fiscal year.

88.2 The ICT DR Plan must be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.

88.3 Within any calendar year, the following test requirements are considered to be minimal:

- Follow the Implementation Plan as provided in the ICT Test Plan;
- At least one Simulation Lite test; and
- At least one other test as defined in the Test Plan.

89. POLICY: ICT DR Team

89.1 The core team of highest priority, is the ICT DR Team (of approximately 10+ roles) of which the key roles that carry the highest effort of responsibility, ultimately responsible for all aspects of Disaster prevention and Disaster recovery, are:

- ICT DR Team Leader; and

- ICT Manager.

89.2 The structure, roles and responsibilities of the ICT DR Team is defined in the ICT DR Plan. These roles must be delegated to key individuals within the Municipality as advised and guided by the ICT DRP.

89.3 This team does not exist as a day-to-day ongoing business entity, but the members come together as a virtual team, to orchestrate all matters relating to an actual or potential Disaster. The team is responsible for the ongoing task of Disaster recovery planning, maintenance of the ICT DR Plan, including the implementation of Disaster prevention activities.

89.4 The ICT Manager and Test team must take considerable care during any test, that possible impact to business operations is investigated prior to the start of the text and checked with Line Managers and Applications Owners.

90. IMPLEMENTATION ROADMAP

Actions- Year One	M1	M2	M3	M4	M5
Convene a KickOff workshop with key personnel to introduce the 5 main documents. Delegate responsibilities.					
Conduct Business Impact/Risk Analysis with Line Managers & Application owner(s)					
Prepare an initial draft of Definition of DR Architecture document by base-lining the current environment.					
Review gaps between the Municpal requirements for DR and the ICT DR Plan & Defn of ICT Arch documents. Update documents.					
Drive initiatives to upgrade DR capability (systems, documents, awareness, RACI.					
Address gaps in ICT DR Plan and Definition fo Architecture documents and update using as-built information.					
Testing - (see ICT DR TestPlan) .					
Identify gaps & assign tasks to improve ICT DR Plan.					
Review policy, audit preparation.					
Actions- Years Two and Three	**M1**	**M2**	**M3**	**M4**	**M5**
Convene a annual DR KickOff workshop with key personnel. Check responsibilities & assign roles.					
Review the Business Impact and Risk Analysis (Line Managers & App Owners).					
Review and improve Definition of ICT DR Architecture.					
Review gaps between Municpal requirements and the ICT DR Plan & Defn oif ICT Arch documents. Update documents.					
Drive initiatives to upgrade DR capability (systems, technology, awareness, RACI).					
Testing - (see ICT DR TestPlan) .					
Identify gaps & assign tasks to improve ICT DR Plan.					
Review policy, audit preparation.					

ICT Data Backup and Recovery Policy

TABLE OF CONTENTS

Glossary of Abbreviations

Abbreviation	Description
AD	Active Directory
HR	Human Resources
UI	User Information
LTO	Linear Tape Open

Glossary of Terminologies

Terminology	Definition
Ad hoc	As and when requested.
Availability	The proportion of time a system is in a functioning condition.
Backup time window	Time slot during a 24hour day that backups are allowed to run in.
Battle box	A battle box is comprised of all the required software and detailed documented information per application, server or data set on how to recover the service in the case of a disaster at the main site.
Critical data	Data that is required to be retained for a set period as determined by law, or data that can severely disrupt services when lost. Examples include: financial data, client personal data etc.
Data medium	Medium on which backups are stored egg. Tapes, hard disks, CD/DVD etc.
Data referencing	Data that defines the set of permissible values to be used by other data sets.
Downtime	Defined as the periods when a system is unavailable.
Generations	Structural term designating the grandfather-father-son (Full-differential-incremental) backup relationship.
Integrity	Data integrity is defined as is the assurance that data is consistent and correct.
Pseudo generation	Randomly created.
Storage capacity	Amount of space (Tb; Gb; Mb) utilized.

1. INTRODUCTION

Information security is becoming increasingly important to the Municipality, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that the Municipality's ICT systems, data and infrastructure are protected from risks such as unauthorised access (see ICT User Access Management Policy for further detail), manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

2. LEGISLATIVE FRAMEWORK

The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

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

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996.
- 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
- Promotion of Administrative Justice Act, Act No. 3 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 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
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- King Code of Governance Principles, 2009

3. OBJECTIVE OF THE POLICY

The primary objective of the policy is to protect the Municipality's data. This policy seeks to outline the data backup and recovery controls for Municipal employees so as to ensure that the data is correctly and efficiently backed up and recovered in line with best practice.

4. AIMS OF THE POLICY

The aim of this policy is to ensure that the Municipality conforms to a standard backup and recovery control process in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency. In addition it seeks to define controls to enforce regular backups and support activities, so that any risks associated to the management of data backups and recovery are mitigated. This policy supports the Municipality's Corporate Governance of ICT Policy.

5. SCOPE

This ICT Data Backup and Recovery Policy has been created to guide and assist the Municipality to align with internationally recognised best practices, regarding data backup, recovery controls and procedures. This policy recognizes that municipalities are diverse in nature, and therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of data backup and recovery.

The policy applies to everyone in the Municipality, including its service providers and consultants. This policy is regarded as crucial to the effective protection of data, of ICT systems of the Municipality. Municipalities must develop their own Data Backup and Recovery controls and procedures by adopting the principles and practices put forward in this policy.

6. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the Municipality and evaluated on its level of severity. Appropriate disciplinary action or punitive recourse will be instituted against any employee or service provider, who contravenes this policy.

Actions include, but are not limited to:

- Revocation of access to Municipal systems and ICT services;
- Disciplinary action in accordance with the Municipal policy; or
- Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978).
- Punitive recourse against a service provider.

7. ADMINISTRATION OF POLICY

The ICT Manager is responsible for maintaining this policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and changes approved by the Council.

8. DATA BACKUP STANDARDS

8.1 Critical data, which is critical to the Municipality, must be defined by the Municipality and must be backed up.

8.2 Backup data must be stored at a location that is physically different from its original creation and usage location, along with a “battle box”.

8.3 Data restores must be tested monthly (see attached template in Appendix: E).

8.4 Procedures for backing up critical data and the testing of the procedures must be documented. These procedures must include, as a minimum, for each type of data:

(a) A definition of the specific data to be backed up;

(b) The type(s) of backup to be used (e.g. full backup, incremental backup, etc.);

(c) The frequency and time of data backup;

(d) The number of generations of backed up data that are to be maintained (both on site and off site);

(e) Responsibility for data backup;

(f) The storage site(s) for the backups;

(g) The storage media to be used;

(h) Any requirements concerning the data backup archives;

(i) Transport modes; and

(j) Recovery of backed up data.

9. DATA BACKUP SELECTION

9.1 All data and software essential to the continued operation of the Municipality, as well as all data that must be maintained for legislative purposes, must be backed up.

9.2 All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.

9.3 The application owner, together with the ICT Manager, will determine what information must be backed up, in what form, and how often (by application of the Backup Types template, Appendix D).

10. BACKUP TYPES

10.1 Full backups should be run weekly as these datasets will be stored for a longer time period. This will also aid in ensuring that data can be recovered with the minimal set of media used at that time. Once a month, a full backup should be stored off site. This statement will need to be reviewed once the ICT DR Business Impact and Risk Analysis requirements are updated with input from Line Managers and Municipal operations.

10.2 Differential/Incremental backups must be used for daily backups. This ensures that the backup time window is kept to a minimum during the week while allowing for maximum data protection.

10.3 In the event that a system requires a high degree of skill to recover from backup, consider taking full images of the servers as a backup. This will ensure that the system can be recovered with minimal knowledge of the system configuration.

10.4 A summary of backup types, along with their advantages, disadvantages and frequency can be found in Annexure D.

11. BACKUP SCHEDULE

11.1 Choosing the correct Backup Schedule:

(a) Backup schedules must not interfere with day to day operations. This includes any end of day operations on the systems.

(b) A longer backup window might be required, depending on the type of backups chosen.

11.2 Frequency and time of data backup:

(a) When the data in a system changes frequently, backups needs to be taken more frequently to ensure that data can be recovered in the event of a system failure.

(b) Immediate full data backups are recommended when data is changed to a large extent or the entire database needs to be made available at certain points in time. Regular, as well as event-dependent intervals, need to be defined.

11.3 Previous versions:

(a) The previous two versions of operating systems and applications must be retained at the off-site storage location.

(b) Annual, monthly and weekly backups must be retained at the off-site facility. Monthly backups may be re-used to take new backups, when annual backups are successfully taken.

12. DATA BACKUP PROCEDURES

12.1 The ICT Manager/team must choose between automated and manual backup procedures based on their requirements and constraints. Both procedures are in line with best practice. The table below outlines the two procedures with their advantages and disadvantages:

Type	Detail	Advantages	Disadvantages
Manual Backups	Manual triggering of the backup procedures.	The operator can individually select the interval of data backup based on the work schedule.	The effectiveness of the data backup is dependent on the discipline and motivation of the operator.
Automatic Backups	Triggered by a program at certain intervals.	The backup schedule is not dependent on the discipline and reliability of an operator.	There is a cost associated with automation. The schedule needs to be monitored and revised to include any non-standard updates and/or changes to the work schedule.

Figure 6 : Advantages and disadvantages of manual and automated backups

12.2 The ICT Manager/team must choose between centralized and decentralized backup procedures based on their requirements and constraints. Both procedures are in line with best practice. The table below outlines the two procedures with their advantages and disadvantages:

Type	Detail	Advantages	Disadvantages
Centralized Backups	The storage location and the performance of the data backup are carried out on a central ICT system by a small set of trained administrators.	Allows for more economical usage of data media.	There is added exposure to confidential data. Confidential and non-confidential information may be combined requiring more stringent security controls for handling the backups.
Decentralized Backups	Performed by ICT users or administrators without being transferred to a central ICT system.	ICT users can control the information flow and data media, especially in the case of confidential data.	The consistency of data backup depends on the reliability and skill level of the user. Sloppy procedures can result in data exposure or loss.

Figure 7 : Advantages and disadvantages of centralized and decentralized backup procedures

13. STORAGE MEDIUM

13.1 When choosing the data media format for backups, it is important to consider the following:

(a) Time constraints around identifying the data and making the data available;

(b) Storage capacity;

(c) Rate of increasing data volume;

(d) Cost of data backup procedures and tools vs. cost if restored without backup;

(e) Importance of data;

(f) Life and reliability of data media;

(g) Retention schedules; and

(h) Confidentiality and integrity.

13.2 Should high availability be required, a compatible and fully operational reading device (e.g. tape drive, CD, DVD) must be obtainable on short notice to ensure that the data media is usable for restoration even if a reading device fails.

14. DATA BACKUP OWNER

14.1 The ICT Manager must delegate a dedicated official, from existing personnel to commit and adhere to each backup schedule.

15. OFFSITE STORAGE SITE

15.1 Data backups must be stored in two locations:

(a) One on-site with current data in machine-readable format in the event that operating data is lost, damaged or corrupted; and

(b) One off-site to additionally provide protection against loss to the primary site and on-site data.

15.2 Off-site backups must be a minimum of 6 kilometres from the on-site storage area in order to prevent a single destructive event from destroying all copies of the data.

15.3 Should high availability be required, additional backup copies should be stored in the immediate vicinity of the ICT system.

15.4 Minimum requirements are to store the weekly, monthly and or yearly backup sets off site.

15.5 The site used for storing data media off-site must meet Physical Security requirements defined within the ICT Security Controls Policy

15.6 Weekly and monthly backups must be stored offsite for the entire duration of the retention period.

15.7 Receipts of media being collected and delivered must be kept for record keeping purposes and must be signed by ICT staff in attendance.

15.8 Should an off-site media set be required to perform a restore, the data media must be returned to the offsite facility for the remainder of the retention period

15.9 All data media used to store confidential information must be disposed of in a manner that ensures the data is not recoverable.

16. TRANSPORT MODES

16.1 When choosing the transport mode for the data (logical or physical), it is important to consider the following:

(a) Time constraints;

(b) Capacity requirements; and

(c) Security and encryption.

17. RETENTION CONSIDERATIONS

17.1 Data should be retained in line with current legislative requirements, as defined in sections 19 and 20 of this document.

17.2 An example of a possible retention schedule is as follows:

(a) A full system backup will be performed weekly. Weekly backups will be saved for a full month.

(b) The last full backup of the month will be saved as a monthly backup. The other weekly backup media will be recycled by the backup system.

(c) Monthly backups will be saved for one year, at which time the media will be reused.

(d) Yearly backups will be retained for five years and will only be run once a year at a predetermined date and time.

(e) Differential or Incremental backups will be performed daily. Daily backups will be retained for two weeks. Daily backup media will be reused once this period ends.

18. RECOVERY OF BACKUP DATA

18.1 Backup documentation must be maintained, reviewed and updated periodically to account for new technology, business changes, and migration of applications to alternative platforms. This includes, but is not limited to:

(a) Identification of critical data and programs; and

(b) Documentation and support items necessary to perform essential tasks during a recovery process.

18.2 Documentation of the restoration process must include:

(a) Procedures for the recovery

(b) Provision for key management should the data be encrypted.

18.3 Recovery procedures must be tested monthly.

18.4 Recovery tests must be documented and reviewed by the ICT Manager.

19. THE ROLE OF BACKUPS IN RECORDS MANAGEMENT

19.1 The National Archives and Records Service of South Africa Act, Act 43 of 1996 requires sound records management principles to be applied to electronic records and e-mails created or received in the course of official business and which are kept as evidence of the Municipality's functions, activities and transactions. The detail of these requirements can be found in:

(a) The [Records Management Policy], [Internet and e-Mail Usage], [Web Content Management Policy] and [Document Imaging Policy] of the Municipality; and

(b) The National Archives and Records Service of South Africa Regulations.

19.2 The Records Manager is responsible for the implementation of sound records management principles and record disposal schedules for the Municipality. The Records Manager is also responsible for maintaining the retention periods indicated on the file plan and disposal schedule.

19.3 The ICT Manager must work with the Records Manager to ensure that public records in electronic form are managed, protected and retained for as long as they are required.

19.4 Backups are not ideal, but not excluded, as a means of electronic record and e-mail retention for the prescribed periods. It is difficult to implement a proper file plan using backup media and therefore it is difficult to arrange, retrieve and dispose of records.

19.5 The role of backups in records management is more suited as a means to recover electronic records management systems and e-mail systems in the event of a disaster or technology failure.

19.6 The ICT Manager is responsible for the following, when backing up electronic records or e-mails that are regulated under the National Archives and Records Service of South Africa Act:

(a) Backups must be made daily, weekly and monthly;

(b) Backups must cover all data, metadata, audit trail data, operating systems and application software;

(c) Backups must be stored in a secure off-site environment;

(d) Backup files of public records must contain the subject classification scheme if files need to be retrieved from the backups;

(e) Backups must survive technology obsolescence by migrating them to new hardware and software platforms when required. An additional option to ensure that data can be read in the future is to store electronic records and e-mails in a commonly used format e.g. PDF or XML.

(f) The backup and retrieval software must also be protected to be available in the event of a disaster;

(g) Backups must be included in disaster recovery plans;

(h) The integrity of backups must be tested using backup test restores and media testing.

19.7 The ICT Manager must ensure that systems prevent the deletion of electronic records or e-mails without consulting the Records Manager.

19.8 The ICT Manager and Records Manager must implement the most practical method to retain e-mails e.g. file inside e-mail application, transmit to document management solution, transfer to e-mail archiving solution, save to shared network drive, print to paper etc.

19.9 Officials are responsible for filing e-mails. It is the responsibility of the sender or their designated official to file e-mails unless the e-mail is received from outside in which case the recipient or designated official is responsible for filing it. The figures below assists with determining responsibility for retaining e-mail messages.

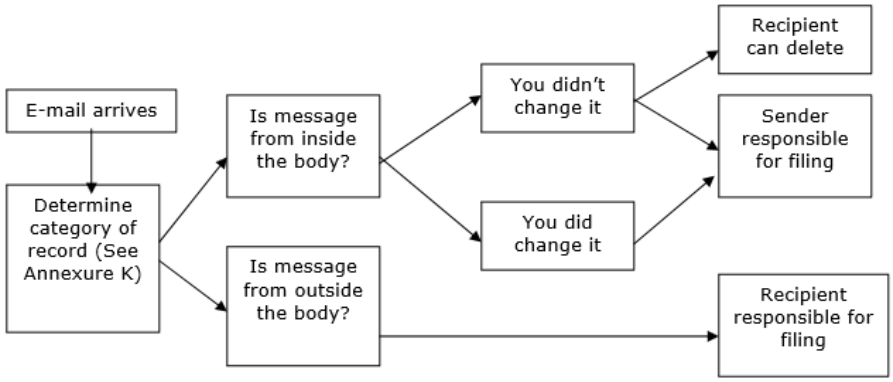


Figure 8 : Example decision sequence to assist with determining responsibility for retaining e-mail messages

(Source: National Archives. Managing electronic records in governmental bodies: Policy, principles and requirements National Archives)

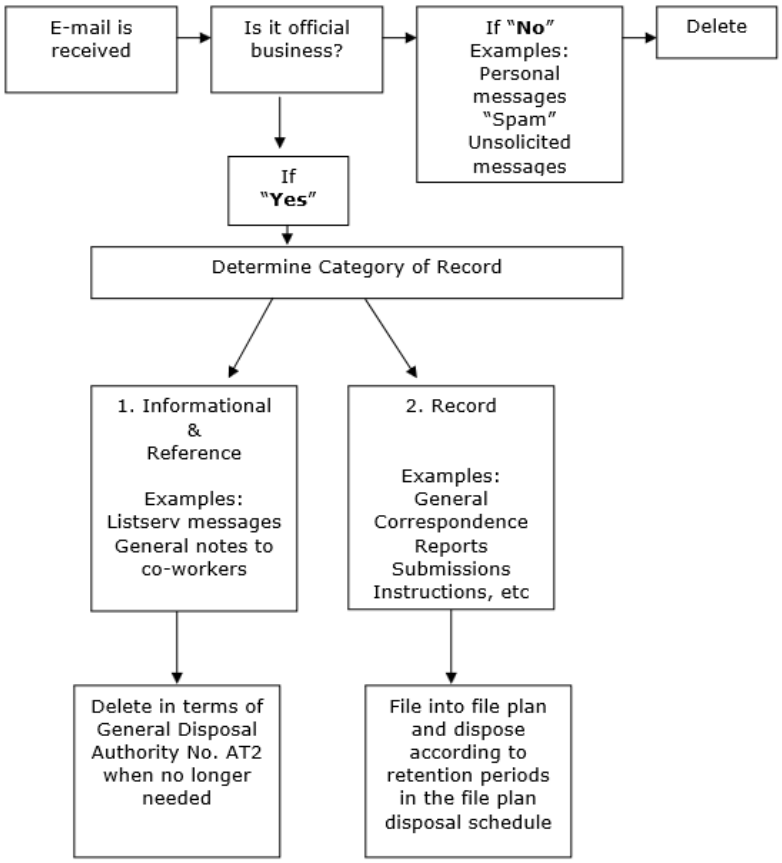


Figure 9 : Examples of a decision sequence for determining e-mail retention

(Source: National Archives. Managing electronic records in governmental bodies: Policy, principles and requirements National Archives)

19.10 The Records Manager must create awareness with Officials of the importance of e-mail as public records. This include, but are not limited to:

(a) E-mails must be properly contextualised and meaningful over time;

(b) Subject lines are very important and must be descriptive;

(c) The reference number of the subject folder in the file plan must be included in the top right hand corner of the message box;

(d) Auto-signatures must be used and shall contain full details of the sender; and

(e) Attachments must be filed into the file plan in the document management system before it is attached to the e-mail.

19.11 The ICT manager must ensure that the e-mail system is set up to capture the sender and the recipient(s), and the date and time the message was sent and/or received. When an e-mail is sent to a distribution list, information identifying all parties on the list must be retained for as long as the message is retained.

19.12 The Records Manager may dispose of any electronic records and e-mails if retention is not required under any Act or General Disposal Authority.

20. GENERAL RULES FOR RETENTION PERIODS

20.1 The National Archives provides the primary considerations when defining retention periods of electronic records and e-mails. This also support the goals of the Promotion of Administrative Justice Act. This supports the goals of the Promotion of Administrative Justice Act, Act. No. 3 of 2000, which is to ensure that public records are available as evidence to ensure that administrative action is lawful, reasonable and procedurally fair.

Act or National Archive Regulations and Guidance	Item	Retention period
National Archives and Record Service of South Africa Act, Act No. 43 of 1996 Promotion of Administrative Justice Act, Act No. 3 of 2000	Public records and e-mails created or received in the course of official business and which are kept as evidence of the Municipality's functions, activities and transactions.	Records may not be disposed of unless written authorisation have been obtained from the National Archivist or a Standing Disposal Authority have been issued by the National Archivist against records classified against the file plan.
General Disposal Authority PAP1 Disposal of personal files of local authorities	Personal case files of local authorities	At the discretion of the Municipality, taking into consideration any special circumstances.
General Disposal Authority No. AE1 for the destruction of ephemeral electronic records and related documentation	Electronic records with no enduring value	16 Categories of records. Refer to AE1 for details.
General Disposal Authority No. AT2 on the destruction of transitory records of all governmental bodies	Electronic records not required for the delivery of services, operations, decision-making or to provide accountability	Refer to AT2 for details.
Managing electronic records in governmental bodies Policy, principles and requirements Managing electronic records in governmental bodies Metadata requirements	E-mails, and attachments therein, must be retained if they: • Are evidence of Municipal transactions; • Approve an action, authorize an action, contain guidance, advice or direction; • Relate to projects and activities being undertaken, and external stakeholders; • Represent formal business communication between staff; or • Contain policy decisions.	E-mails fall into one of the 4 categories above and must be retained as such.

Figure 10 : Retention periods specified by the National Archives

20.2 Public records that are needed for litigation, Promotion of Access to Information requests or Promotion of Administrative Justice actions may not be destroyed until such time that the Legal Services Manager has indicated that the destruction hold can be lifted.

20.3 The Municipal Finance Management Act, No 56. of 2003, Section 62 1)b) states that Municipal records must be retained in the manner prescribed by legislation. However, the Act does not specify retention periods. National and Provincial retention periods for financial records are prescribed within Treasury Regulations, Regulation 17 to the Public Finance Management Act, No. 1 of 1999, Section 40(1)(a). For the purposes of this policy, the Treasury Regulations, Regulation 17, will be used as guidance only without intervening National Archivist legislation, regulations and guidance.

Act or National Archive Regulations and Guidance	Item	Retention period
Treasury Regulations, Regulation 17	Internal audit reports, system appraisals and operational reviews.	10 years
Treasury Regulations, Regulation 17	Primary evidentiary records, including copies of forms issued for value, vouchers to support payments made, pay sheets, returned warrant vouchers or cheques, invoices and similar records associated with the receipt or payment of money.	5 Years
Treasury Regulations, Regulation 17	Subsidiary ledgers, including inventory cards and records relating to assets no longer held or liabilities that have been discharged.	5 Years
Treasury Regulations, Regulation 17	Supplementary accounting records, including, for example, cash register strips, bank statements and time sheets.	5 Years
Treasury Regulations, Regulation 17	General and incidental source documents not included above, including stock issue and receivable notes, copies of official orders (other than copies for substantiating payments or for unperformed contracts), bank deposit books and post registers.	5 Years

Figure 11 : Retention periods specified by Treasury Regulations, Regulation 17 (guidance only)

20.4 In accordance with Treasury Regulations, Regulation 17(2), financial information must be retained in its original form for one year after the financial statements and audit report has been presented to the Council.

20.5 Financial information may be stored in an alternative form, after expiry of one year from submission of the financial statements to the Council, under the following conditions:

(a) The records must be accessible to users. This requires data referencing, a search facility, a user interface or an information system capable of finding and presenting the record in its original form.

(b) The original form may have reasonable validations added, which is required in the normal course of information systems communication, storage or display.

20.6 The Electronic Communication and Transaction Act, No 25 of 2005 regulates the storage of personal information:

Act	Item	Retention period
Electronic Communication and Transaction Act, No 25 of 2005	Personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information.	As long as information is used, and at least 1 year thereafter.
Electronic Communication and Transaction Act, No 25 of 2005	A record of any third party to whom the information was disclosed must be kept for as long as the information is used.	As long as the information is used and at least 1 year thereafter.
Electronic Communication and Transaction Act, No 25 of 2005	All personal data which has become obsolete.	Destroy

Figure 12 : Retention periods specified by the Electronic Communication and Transaction Act, No 25 of 2005

20.7 The Protection of Personal Information Act, No. 4 of 2013 ("POPI") will regulate the retention of personal information when it becomes active:

Sections	Item	Retention period
Sections 9 to 18	Gender, sex, marital status, age, culture, language, birth, education, financial, employment history, identifying number, symbol, e-mail address, physical address, telephone number, location, online identifier, personal opinions, views, preferences, private correspondence, views or opinions about a person, or the name of the person if the name appears next to other personal information or if the name itself would reveal personal information about the person.	Do not collect or retain unless the person have been given notice and consent obtained. Exceptions apply. Personal information may not be retained for longer than agreed with the person, unless the retention of the record is required by a law. (This principle is applicable to all items in this table. The retention of items that follow is expressly prohibited unless exceptions apply.)
Sections 6, 34 to 37	Children's information	Destroy unless, exceptions apply e.g. establishment or protection of a right of the child.
Sections 6 & 28	Religious or philosophical beliefs	Destroy unless, exceptions apply e.g. to protect the spiritual welfare of a community.

Sections	Item	Retention period
Sections 6 & 29	Race or ethnic origin	Destroy unless, exceptions apply e.g. protection from unfair discrimination or promoting the advancement of persons.
Sections 6 & 30	Trade union membership	Destroy unless, exceptions apply e.g. to achieve the aims of trade union that the person belongs to.
Sections 6 & 31	Political persuasion	Destroy unless, exceptions apply e.g. to achieve the aims of a political institution that the person belongs to.
Sections 6 & 32	Health or sex life	Destroy unless, exceptions apply e.g. provision of healthcare services, special support for pupils in schools, childcare or support for workers.
Sections 6 & 33	Criminal behaviour or biometric information	Destroy unless, exceptions apply e.g. necessary for law enforcement.

Figure 13 : Retention periods specified by the Protection of Personal Information Act, No. 4 of 2013

21. ANNEXURE A: IMPLEMENTATION ROADMAP

No	Action	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10
1	Review current backup and recovery procedures										
2	Assess compliance to ICT Data Backup and Recovery Policy										
3	Implement changes to procedures										
4	Train staff in new procedures										
5	Test newly implemented procedures										

22. ANNEXURE B: IMPLEMENTATION GUIDE

The Municipality will need to standardise its backup solution and backup medium across all sites to implement the policy. The backup medium may include data replication to another site. Off-site storage of the backups may therefore be

A supplier must be selected to cater for off-site storage of backups if another government entity will not be used.

Where possible, the below strategy must be strictly adhered to:

	Full Backup			Differential Backup	Incremental Backup
Data Set	**Monthly**	**Weekly**	**Yearly**	**Daily**	**Daily**
Financial Systems	Last weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	
HR Systems	Last weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	
File and Print	Last weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	Monday to Friday
Business Enablers (Mail, AD etc.)	Last weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	
Security Access	Last weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	
Supporting Material (Application installation files)	Last weekend in the month	Last day of the week	Weekend after Financial Year end	Monday to Friday	

Figure 14 : Example backup strategy

23. ANNEXURE C: TEMPLATE EXAMPLES

Backup Component	Responsible	Accountable	Contribute	Inform
Data Criticality "Rating"	ICT Application Team	ICT Application Team	ICT Team	ICT Backup Operator
Detailed Application/Server Build Documentation	ICT Application Team	ICT Team	ICT Backup Operator	ICT Backup Operator
Data Backup Selection List	ICT Team	ICT Application Team	ICT Backup Operator	ICT Backup Operator
Backup Monitoring	ICT Backup Operator	ICT Backup Operator	ICT Team	ICT Application Team
Backup Reporting	ICT Backup Operator	ICT Backup Operator	ICT Team	ICT Application Team
Media management	ICT Backup Operator	ICT Backup Operator	ICT Team	ICT Application Team
Offsite Storage	Offsite Data Custodians	ICT Backup Operator	ICT Team	ICT Application Team

Figure 15 : Example roles and responsibilities

Backup Component	Daily	Weekly	Monthly	Quarterly	Ad hoc
Selection List Modifications					X
Backup Monitoring	X				
Backup Reporting		X	X		
Backup Capacity Reporting		X	X		
Backup Media Handling	X	X	X		
Restore Testing				X	

Figure 16 : Example backup timeline

No	Item	Action

System being backed up	Data Classification: Business critical data Server role: File and print server
Backup Selection	The data required to be backed up is determined and identified by the owner of the data set on this server.
Media used	• Tape library with LTO 6 tapes • No data encryption enabled
Backup Schedule	• Daily backups: Runs Monday – Friday from 18:00 – 23:00 • Weekly backups: Runs every Saturday from 18:00 – 23:00 • Monthly backups: Runs on the last Saturday of the month from 18:00 – 23:00 and replaces the Weekly backup for this scheduled period. • Yearly backup: Is manually run after financial yearend
Data Retention	• Daily backups: Media set is retained for 2 weeks • Weekly backups: Media set is retained for 1 month • Monthly backup: Media set is retained for 1 year • Yearly backup: Media set is retained for 5 years
Offsite Storage	• All media is moved and stored offsite at a secured facility after the successful completion of the backup. • The same facilitator providing the offsite storage, is used to provide transport of the media to the secure site.
Data Backup Owner	• The backup is monitored and media is inserted on a daily basis by 2 identified onsite contacts.

Figure 17 : Example backup strategy for a system

24. ANNEXURE D: BACKUP TYPES

Type	Detail	Advantages	Disadvantages	Frequency
Full data backup	All data requiring backup is stored on an additional data medium without considering whether the files have been changed since the last backup.	Simple and quick restoration of data due to the fact that all relevant and necessary files can be extracted from the latest full data backup.	Requires a high storage capacity. If full data backups are not carried out regularly, extensive changes to a file can result in major updating requirements.	Weekly and monthly.
Incremental data backup	This procedure stores the files which have been changed since the last incremental/full backup. Incremental data backups are always based on full data backups and must be combined periodically with full data backups. During restoration, the latest full backup is restored first, after which incremental backups are restored to the most current state of the backed-up data.	Saves storage capacity and shortens the time required for the data backup.	Restoration time for data is generally high, as the relevant files must be extracted from backups made at different stages.	Daily.
Differential data backup	This procedure stores only the files that has been changed since the last full data backup. During restoration, the latest full backup is restored first, after which differential backups are restored to the most current state of the backed-up data.	Files can be restored quicker and easier then incremental backups.	Requires more capacity on the backup medium than an incremental backups.	Daily.
Image backup	This procedure backs up the physical sectors of the hard disk rather than the individual files on it.	Full backup which allows for very quick restoration of hard disks of the same type. Very effective for disaster recovery.	Not useful for restoration of individual files.	Used for systems with very specific and specialized configuration.

Figure 18 : Advantages and disadvantages of backup types

25. ANNEXURE E: RESTORE TESTING TEMPLATE

RESTORE TESTING TEMPLATE

a) *Responsible person:* *b)* *Location / dept.:*

c) *Date:*

SERVER BACKUPS TESTED:

1.☐ *server OS: ……*

2.☐ *server OS: ……*

3.☐ *server OS: ……*

4.☐ *server OS: ……*

5.☐ *server OS: ……*

DATABASE BACKUPS TESTED:

1.☐ *database: ……*

2.☐ *database: ……*

3.☐ *database: ……*

4.☐ *database: ……*

5.☐ *database: ……*

OTHER BACKUPS TESTED:

1.☐ *Other: ……*

OFF-SITE BACKUPS TESTED:

1.☐ *server OS: ……*

2.☐ *server OS:: ……*

3.☐ *database: ……*

4.☐ *database: ……*

DATABASE REPLICATION TESTED:

1.☐ *: ……*

☐ *Backups can be used for disaster recovery*

h) Reviewed: *i) Date:* .

26. ANNEXURE E: REFERENCES

BS ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls. (2013). Geneva: BSI Standards Limited.

Control Objectives for Information Technology (COBIT) 5. (2012). Illinois: ISACA.

Electronic Communications and Transactions Act, No. 25. (2002). Republic of South Africa.

King Code of Governance for South Africa. (2009). Institute of Directors in Southern Africa.

Local Government: Municipal Finance Management Act, No. 53. (2003). Republic Of South Africa.

Minumum Information Security Standards. (1996, December 4). Cabinet.

Protection of Personal Information Act, No. 4. (2009). Republic of South Africa.

Treasury Regulations for departments, trading entities, constitutional institutions and public entities. (2005, March). National Treasury, Republic of South Africa.

STANDARD OPERATING PROCEDURES

TABLE OF CONTENTS

1. Introduction

Standard Operating Procedures (SOP) are a vital management feature in Information Technology management. All approved ICT policy documents should be accompanied by approved SOP statements that drive best practice activity schedules. These SOPS tables will assist ICT Managers and supporting staff to drive continuous service quality, teamwork, department performance and over time, elevate the ICT team profile within the Municipality.

2. ICT Operations Daily Checklists

Name:																	
Designation:																	
	Month /Week																
Daily Check List	Date	Date	Date	Date	Date	Date	Date	Date	Date	Date	Date	Date	Date	Date	Date	Date	**Manager's Signature**
General Daily Checklist																	
Verify that the exchange database is mounted																	
Make sure that public folders replication is up to date																	
Check the mailbox size for each user																	
Check the message queues																	
Check anti-Virus for updates																	
Verifying that the previous backup operations were completed																	
Analyse and attend to errors during backup																	
Follow procedures for tape rotation and off-site storage																	
Check Server room Temperature environment																	
Make sure that security measures are in place(Locks, access codes)																	
Ensure that the Operating Network is Operational (network ,routers, switches)																	
Ensure telephony architecture is functional																	
Check all server hardware for faults and errors																	

Respond to discovered failures and problems																
Make sure all access points are online and broadcasting																
Establish connection and access shares from each access point																
Trouble shoot all faulty points																
Make sure all network printers are online																
Troubleshoot all offline printers and copiers																
Attend to ICT requests																
Check vendors for device updates/patches & hotfixes																
ICT Security Controls SOP Check List																
Operate the change control process																
Examine major events logged on the firewall																

3. ICT Operations Weekly Checklists

Name:					
Designation:					
	Month				
Weekly Check List	**WEEK 1**	**WEEK 2**	**WEEK 3**	**WEEK 4**	**Manager's Signature**
General SOP					
Ensure backups are stored off site					
Verify restore operational by restoring test files weekly					
Check for the latest Software updates for all servers					
Check for the latest Hardware updates for all servers					

Check for software updates for all network hardware					
Approve and install any new updates					
Weekly Report on uptime on all servers					
Weekly report on uptime of Network					
Weekly report on Uptime of Telephony infrastructure					
Weekly report on internet usage					
ICT Security Controls SOP					
Check updates and patches for network equipment					
Create weekly change control report					
Review change control report and take action					
Monitor changes recently implemented					
Review completed change requests and close					
Update records on security incidents					

4. ICT Operations Monthly Checklists

Name:		
Designation:		
	Month	
Monthly Check List	**Comments**	**Manager's Signature**
General SOP		
Do test restore on all environments for backups		
Note repetitive warnings and errors on Server Error Logs		
Update site file for any changes to servers		
Monthly Uptime Report		
Monthly report on uptime of Network		
Monthly report on Uptime of telephony infrastructure		
Monthly report on internet usage		

Monthly report on Intrusion detection		
Receive terminated user list from HR		
Perform user termination review		
Perform all users review with administrative access		
Review user access logs		
ICT SLA SOP		
Review service levels of Strategic and Tactical contracts		
Inform ICT Steering Committee of service delivery failures on Strategic and Tactical contracts		
Escalate continued service delivery failures to the ICT Steering Committee at their next scheduled meeting		
Communicate unsatisfactory performance to service providers/vendors in writing		
Update agreements with changes to outsourced ICT services		
Ensure that service providers/vendors follow the change control process		
Progress actions to deal with ICT internal service level failures		
ICT Security Controls SOP		
Scan the internal and external network for vulnerabilities with security software		
Examine significant events logged on the security devices		
ICT DR SOP		
Monthly meetings to review status of document, changes to future state (planned or implemented) & actions to update document Invite Application owners and Municipal Line Managers		
Monthly report of ICT all DR activity, improvements, changes & issues to ICT DR Team Leader		
Compile a **ICT DR Planning Risk register and a separate project initiatives programme summary** (name, outcome, supplier, durations, effort and costs, explain key dependencies)		
IT Manager to **consult with ICT DR Team leader** to address any identified gaps in technologies & architecture (e.g. after ICT DR testing)		
Meet with **Applications Owners, Line Managers, and Municipal Manager** to check if Business Requirements (risk, prioritisation, impact) have changed requirements, and if the technologies and Architecture are still “fir for purpose” and ready for testing		
Ensure that **ICT supplier contracts** (focus on services more than solution) are up to date, to check if ready for next iteration of testing		

Update ICT DR Definition of Architecture document, with input from key technology experts, if required Update Roadmap for major changes in technology planning Check & record key dependencies by consultation with experts		
Provide input into reporting to the Council on the **performance of the suppliers** if requested		
Assess the suppliers' solutions and contracts, to identify opportunities to save costs or use alternative suppliers		
DR Policy SOP		
One Progress meeting across the ICT DR framework of documents		
Check if Business Impact and Risk Analysis is complete, with version control and signed-off		
Check with Change Management owner if and what major changes have occurred that will impact the ICT DR capability		
Check and approve what testing is intended for the year, aligning with Municipal Manager and Line Managers		
Check the involvement and key delivery of capability, and approvals with 3rd party Suppliers		
Contact any offsite DR contact persons to check status – all communication should be minuted, and key email stored and/or archived		
Provide a high level report of the ICT DR capability to management		
Highlight changes to policy for an annual review		
ICT DR Plan SOP		
One Progress meeting across the ICT DR framework of documents		
Check if Business Impact and Risk Analysis is complete, with version control and signed-off		
Check with Change Management owner if and what major changes have occurred that will impact the ICT DR capability		
Check and approve what testing is intended for the year, aligning with Municipal Manager and Line Managers		
Check the involvement and key delivery of capability, and approvals with 3rd party Suppliers		
Contact any offsite DR contact persons to check status – all communication should be minuted, and key email stored and/or archived		
Provide a high level report of the ICT DR capability to management		
Highlight changes to policy for an annual review		

5. ICT Operations Quarterly Checklists

Name:		
Designation:		
	Month	
Quarterly Check List	**Comments**	**Manager's Signature**
General SOP		
Review RAS/VPN logs – Systems Administrator		
Review DB rights & permissions – ICT Manager		
Review user permissions – Systems Administrator		
Test compliance of baseline settings – Audit & Risk Committees		
Review compliance exceptions – Risk Committee		
Review access to network shares – Systems Administrator		
Review end-point OS Firewalls rules – Systems Administrator		
ICT SLA SOP		
Review service levels of Operational contracts		
Deal with service delivery failures on Operational contracts		
Update inventory of ICT contracts		
Ensure that all ICT contracts have a contract manager		
Collect data to measure ICT internal service levels		
Submit a report on ICT internal service levels to the ICT Steering Committee		
ICT Security Controls SOP		
Review access to the server room		
Review maintenance schedule for the server room		
Review physical security against policy		
Update network documentation		
Review firewall rulesets		

Review use of personal firewalls		
Review inactive network points and disable		
Review database access against policy		
Review firewall controls against policy		
Review e-mail and Internet security controls against policy		
Review wireless security against policy		
Review mobile device controls against policy		
Review security incidents to identify root causes		
Review and update records of purchased software licenses		
Review and update approved software list		
Review change control against policy		
ICT DR SOP		
High Level meeting with team to review and confirm ICT DR Plan – update versions		
Check planning for ICT DR tests and awareness campaign activity.		

6. ICT Operations Bi-Annual Checklists

Name:		
Designation:		
	Month	
Bi-annual Check List	**Comments**	**Manager's Signature**
General SOP		
DR Architecture updated/or every time environment changes		
ICT SLA SOP		
Strategically re-consider Strategic and Tactical contracts		
Consider soliciting audits of service provider / vendor environments		
ICT DR SOP		

Meet with **Applications Owners, Line Managers, and Municipal Manager** to check if Business Requirements (risk, prioritisation, impact) have changed requirements, and if the technologies and Architecture are still “fir for purpose” and ready for testing		
Update ICT Disaster Recovery Architecture document reflecting any changes in requirements (from BIA updates) and Architecture solution changes.		

7. ICT Operations Annual Checklists

Name:		
Designation:		
	Month	
Annual Check List	**Comments**	**Manager's Signature**
General SOP		
Review of version baselines – Risk & ICT Steering Committees		
ICT SLA SOP		
Ensure that all ICT contracts can be found in the registry		
Strategically re-consider Operational contracts		
Identify ICT service providers/vendors that process personal information		
Review agreements to ensure that personal information is protected		
Review all ICT contracts against prescribed minimum terms		
Review the ICT services catalogue with directorates		
Review ICT services catalogue with the directorates against the IDP and SDBIP		
ICT Security Controls SOP		
Review inventory of personal information		
Review inventory of classified information		
Review inventory of electronic public records		
Review and maintain protection of personal information		

Review and maintain protection of classified information		
Review with Records Manager the protection of electronic public records		
Scan the environment for unauthorised wireless networks		
Scan environment of for installed software		
Compare installed software to licenses		
Remove unlicensed software		
ICT DR SOP		
Initiate a comprehensive BIA analysis with key Line Managers and Application Owners		