MATJHABENG CORPORATE GOVERNANCE FOR INFORMATION, COMMUNICATION AND TECHNOLOGY POLICY

(MCGICTP)

Contents

Document Information

Project Name:	Matjhabeng ICT Governance Framework		
Prepared By:	Matjhabeng ICT	**Document Version No:**	1.3
Title:	ICT Governance Framework	**Document Version Date:**	03/04/2018
Reviewed By:		**Review Date:**	

Distribution List

Name	Date	Phone/Fax/Email

Document Version History

Version Number	Version Date	Revised By	Description	Filename
1.0	10 September 2013	Matjhabeng ICT	Document creation	Matjhabeng ICT Governance Policy
1.1	03 January 2017	Matjhabeng ICT	Second Draft	Matjhabeng ICT Governance Policy
1.2	29/03/2018	Matjhabeng ICT	Update, RACI, Org Structure and alignment to COGTA ICT Governance Framework.	Matjhabeng ICT Governance Policy
1.3	03/04/2018	Matjhabeng ICT	Document update	Matjhabeng ICT Governance Policy

1. INTRODUCTION

1.1 Matjhabeng's ICT

Matjhabeng Local Municipality's information and communications technology ("ICT") lies within the Directorate of Strategic Support Services. ICT within the municipality is essential to manage communications, information and knowledge necessary to ensure service delivery requirements. With all the essential benefits that ICT brings to the municipality, there comes a need to manage risks and to implement a system (ICT Governance Framework) by which the current and future use of ICT is directed and controlled. The framework involves evaluating and directing the plans for the use of ICT to support the organisation and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organisation.

To support the application of these principles, the municipality has decided to establish an ICT governance framework and guideline, which comprises the definition and importance of governance within the public sector, alignment with legislation, requisite standards for municipalities, as well as definition and clarity on decision making mechanisms, amongst others.

1.2 Definitions

The Matjhabeng Corporate Governance ICT Policy (MCGICTP), is an integral part of corporate governance and this document focuses specifically on ICT policies, roles and responsibilities and implementation to ensure that Matjhabeng is aligned to industry best practices along with being compliant to legislative frameworks with the intention of being geared to harnessing and leveraging ICT as a key enabler to support the municipalities' ability to improve service delivery to the community whilst ensuring ICT alignment and satisfaction internally.

This framework is viewed as encompassing the following strands:

- ICT Policy Management
- ICT Budget Management
- ICT Risk Management
- Enterprise Architecture Management

1.3 Scope and Applicability

This framework applies to all divisions and units within the municipality. It focuses on the Matjhabeng ICT policy management lifecycles, as part of a wider ICT governance framework, which is also defined in this document.
This Framework adopts the approach of clarifying principles and objectives to support and sustain effective governance of ICT.

2. Adopted Frameworks

By adopting this framework, the following outcomes are anticipated:

- Raising the profile of ICT within the municipality;
- Raising the profile of ICT as a strategic enabler for effective administration and service delivery;
- Bringing international good practices into the municipality;
- Further strengthening corporate governance of ICT as well as ensuring that ICT is given the strategic priority that is required;
- Institutionalising ICT governance as integral part of municipal corporate governance;
- Setting a framework for ICT governance standards within the local municipality;
- Improving the ICT governance education and awareness levels within the municipality.

Political leadership and executive management of Matjhabeng will extend corporate governance as a good management practice into the ICT space and evaluate, direct and monitor the execution of ICT in line with the Public Service and Institution's strategies.

There are international and national mechanisms available that provide guidance for the implementation of governance of ICT, such as;

2.1 King report on governance for South Africa 2009 (“King III”)

King III is the abbreviated name for the King Report on Government for South Africa Published 2009 in South Africa. It followed a 1994 report commonly known as a King I, and 2002 report commonly known as King II. The King Report on Corporate Governance has been cited as "the most effective summary of the best international practices in corporate governance"

2.2 ISO/IEC 38500

An international standard for corporative governance of information technology published jointly by the International Organisation for Standardisation (“ISO”) and the International Electro-Technical Communication (“IEC”). It provides a framework for effective governance of IT to assist those at the highest level of organisations to understand and fulfil their legal, regulatory, and ethical obligations in respect of their organisation’ s use of IT. This International standard is adopted by South Africa as SANS 38500.

2.3 COBIT 5®

Abbreviation for “Control Objectives for Information and Related Technology”, a set of best practices (framework) for information technology (IT) management created by the Information Systems Audit and Control (ISACA), and the IT Governance Institute (ITGI) in 1996.

The principles and models as explained in the above frameworks and standard has been used to define and describe governance in this framework and to provide the principles of good governance of ICT.

COBIT 5 is the latest edition of ISACA’s globally accepted framework, providing an end-to-end business view of the governance of enterprise IT that reflects the central role of information and technology in creating value for enterprises.

2.4 ITIL V3

The Information Technology Infrastructure Library (ITIL) is a set of concepts and practices for Information Technology Services Management (ITSM), Information Technology (IT) development and IT operations. ITIL describes processes, procedures, tasks and checklists that are not organisation-specific, used by an organisation for establishing integration with the organisation's strategy, delivering value and maintaining a minimum level of competency. It allows the organisation to establish a baseline from which it can plan, implement and measure. It is used to demonstrate compliance and the measure improvement.

3. MUNICIPAL PLANNING CONSIDERATIONS

3.1 Municipal Strategic Planning

The municipality's strategic direction is articulated through the development of strategic, operational and specific purpose plans. Matjhabeng has an integrated business planning, which cascades from the department and district strategic plans through to other municipalities as well as internal divisional plans.

The goals and objectives in the municipality's plans are distilled into each employee's individual performance and development plan. Planning requirements for the municipality are set out in the Integrated Development Plan 2017 – 2022.

3.2 ICT Strategic Plan

Matjhabeng will clearly define a formal ICT Strategic Plan, which aligns with the IDP and will form a key implementation component of Service Delivery Budget Implementation Plan ("SDBIP").

3.3 ICT Operations Plan

Annual operational plans will be developed for the ICT function. Operational plans align to the ICT Strategic Plan and other strategic documents, and outline objectives with related performances measures and risk identification and mitigation strategies.

Operational plans also detail the major programmes and projects being undertaken to meet the objectives. Operational plans are developed through a process of environmental scanning to determine upcoming challenges and new priorities, and reviewing the past year's performance in delivering on identified objectives and performance measures.

4. ENSURING MUNICIPAL ALIGNMENT

4.1 What is organisational alignment

Organisational alignment ensures that all aspects of ICT are aligned with the municipal strategy and operational plans. This involves ensuring that the ICT structures, processes and systems are responsive and aligned with any change in strategic direction and business process within the municipality. It includes the governance mechanisms that empower management and ensure accountability, and the setting and monitoring of performance objectives (performance management).

Successful organisational alignment requires strong commitment from management, and the cascading of this commitment across the municipality. Senior management must model good governance and demonstrate a commitment to achieving objectives through accountability. Effective communication is essential at all levels to ensure congruence and a clear line of sight from the municipality's high-level strategies to individual performance plans.

Line managers are to consistently promote and implement municipal governance processes through clear communication about employees' governance responsibilities, and by incorporating good governance into daily activities and performance management processes. Employees are to be aware of their governance responsibilities and to actively support the municipality's model of strong corporate governance.

4.2 Organisational Structure

Matjhabeng's Organisational Structure, as well as prospective changes thereto, has been designed to ensure effective organisational alignment of functions and operations with the delivery of key services.

The structure achieves this by providing clear lines of reporting, accountability and responsibility to support appropriate, open transparent decision-making processes.

4.3 ICT Governance Committee

The municipality will establish an IT Steering committee to advise and support the Municipal Manager in discharging responsibilities relevant to the ICT space. IT Steering committee terms of reference will be developed to ensure clarity of roles and protocols for members of the committee.

This committee interacts and is supported by other governance committees within the municipality, as relevant. The governance committees provide forums for senior management and members of the committees to engage on a range of governance and performance aspects as well as make recommendations to the Municipal Manager for enhancements thereto.

Benefits of having an IT Steering committee include:

- Gain senior management involvement and support.
- Keeping ICT visible and significant to senior management.
- Maintain access to high-level decision makers.
- Create a cross-functional perspective with representatives from various interests.
- Reach a consensus on issues that cannot be resolved by the day-to-day ICT team.

4.4 Best practice in governance steering committee

The municipality will utilise best practice for establishing and operating its governance committees. Best practice requires attention to the four stages - step-up, operations, follow-through and review.

- Step-up - the purpose, functions, roles and processes for the committee operations, processes and review need to be identified and documented in the set-up phase.
- Operations - the role of an efficient and effective secretariat to work with the chair of a committee in agenda setting and managing the operations of the committee meetings is key to their success in meeting their purpose and function.
- Follow-through - for committees to achieve their objectives, they need to have processes to ensure follow-through of actions or decisions, the escalation of issues to other committees if appropriate, and the communication of key decisions or actions to other governance committees.
- Review - periodic review of committees needs to be undertaken to ensure they are still meeting their intended purpose, gauge their performance, or determine whether their intended purpose is still relevant.

5. COMMITTEE SUMMARY

IT Steering Committees are a best practice approach for aligning strategic business and IT priorities.

Clear mandates and a real ability to influence decision making through executive participation increase the value of IT Steering Committees. Successful IT Steering Committees focus on three main tasks: ICT strategic planning, project prioritisation and project approval. Other activities, such as resource allocation, are best left to the operational teams and management.

The IT Steering committee has amongst its broad range of duties, the duty to get leadership to understand their role in ICT governance and comply thereto using a facilitative role.

6. ACCOUNTABILITY & LEGAL MANDATE

‘Accountability’ is the acknowledgment of responsibility for policies, decisions and actions within the scope of a role. It encompasses the obligation to report, explain and be the answerable for resulting consequences.

6.1 Legislation

In line with CoGTA recommendations for Local Municipality Corporate Governance for ICT the following legislation is applicable:

- 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.

The Constitution of South Africa envisages a robust local government system, which can provide democratic and accountable government for local communities; ensure the provision of services to communities in a sustainable manner; promote social and economic development; promote a safe and healthy living environment; and encourage the involvement of communities and community organisations in matters of local government.

The Municipal Systems Act [No 32 of 2000] defines the legal nature of municipalities as part of a system of co-operative government. It also clarifies the right and duties of the municipal council, local communities, and the municipal administration. Clarifying the rights and obligations of different parties is an important step towards strengthening the democratic contract at the local level.

The Municipal Systems Act clarifies several issues relating to municipal powers, functions and duties. A municipality has all the functions and powers assigned to it in terms of the constitution. It has the right to do anything reasonably necessary for, or incidental to, the effective performance of its functions and the exercise of its powers.

Municipalities exercise their executive and legislative authority in a number of ways, including by developing and adopting policies, plans, strategies and programmes; establishing and maintaining an administration; promoting and undertaking development; setting targets for delivery; providing municipal services or regulating the provision of municipal services; implementing national and provincial legislation and its own by-laws ;preparing, approving and implementing its budgets; as well as setting and collecting services charges amongst others.

6.2 Delegations

The Mayor and the Municipal Manager are given powers under both agency-specific and whole-of-government legislation usually includes a definition of ‘appropriately qualified’, which generally relates to the possession of qualifications, experience or standing appropriate for the function.

Some Acts also enable the delegated officer to sub-delegate the power or function to another officer in the municipality. If the relevant Act does not include a specific power of delegation or sub-delegation, there can be no specific express delegation of a power or the revocation of a delegation must be in writing, signed by the delegator.

6.3 Financial Accountability

The ICT department has an obligation to account for the way resources are allocated and used to ensure that public money is spent economically and efficiently, and that Matjhabeng’s municipal area benefits from government investment. The municipality’s financial governance framework is primarily developed from government legislation, policy and guidelines, and is documented in the Municipal Finance Management Act 56 of 2003. The Municipal Finance based, and requires the municipality, amongst other aspects, to develop and implement systems of internal control, which best its circumstances, while meeting prescribed accountability requirements.

6.4 Information Management

6.4.1 Access to information

The promotion of Access to information Act, No 2 of 2000 was enacted by Government to provide greater community access to information produced in the public sector. The Act ensures equal access to information across all sectors of the community, unless on balance it is contrary to the Public interest to disclose that information.

6.4.2 Information privacy

The protection of personal information Bill [POPI] aims to protect individuals' personal information by organisations. The Protection of Personal Information Act, No 4 of 2013 promotes the protection of personal information by public and private bodies.

The Protection of Personal Information (POPIA) Act has been signed into law on 19 November and published in the Government Gazette Notice 37067 on 26 November 2013.

6.4.3 Corporate reporting

Clear and unambiguous lines of reporting, accountability and responsibility, both within the organisation and with its stakeholders, are critical to effective governance. The ICT department will develop systems of internal and external reporting, which demonstrate its commitment to transparency, accountability and good governance practice.

6.4.4 Corporate governance in the municipality

The municipality adopts the highest standards of governance and expects stakeholders and staff members to align with this principle. The purpose of corporate governance is to create value for stakeholders of the institution. This value creation takes place within a governance system that is established through this framework. It consists of a governance system that affects the way public services institutions are managed and controlled. It also defines the relationship between stakeholders, strategic goals of the municipality and institutions.

A governance system refers to mechanisms that enable multiple stakeholders of an institution to perform or influence the following:

- **Evaluate** internal and external context, strategic direction and risk to conceptualise the institution's strategic goals and how it will be measured.
- **Direct** the institution to ensure that value is realised, and risk is managed.

- To **monitor** the execution of the strategic goals within an institution against the measures identified for attaining the strategic goals. Corporative governance is also concerned with individual accountability and responsibilities within an institution: it describes how the institution is directed and controlled.

  And is in particular concerned with:

- **Organisation –** the organisational structures, and coordinating mechanisms (such as steering forums) established within the institution and in partnership with external bodies;
- **Management –** the individual roles and responsibilities established to manage business change and operational services; and
- **Policies –** the frameworks established for making decisions and the context and constraints within which decision are taken.

6.5 Governance of ICT in the municipality

The governance of ICT is a subset of corporate governance and is an integral part of the governance system within an institution. The governance of ICT is defined as "the system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organisation and monitoring this use to achieve the plans. It includes the strategy and policies for using ICT within an organisation."

The executive authority and management are accountable and responsible to ensure that governance of ICT is implemented in their institution in line with this framework.

Effective governance of ICT is implemented in Matjhabeng by:

- Assigning responsibilities to executive and senior management with decision making authority;
- Utilising appropriate governance mechanisms;
- Aligning ICT goals with business goals and ensure that business benefits are realised, and risk managed;
- Investing in ICT to enable the institution in the realisation of business value;
- Ensuring that appropriate business ownership of ICT projects is established;

- Providing the necessary capacity and capability in ICT to support business programmes;
- Ensuring that ICT is monitored and measured.

The implementation of the governance of ICT can be achieved through the following means and mechanisms:

Means and mechanisms;

- Frameworks;
- Principles;
- Policies;
- Structures.

Decision making mechanisms:

- Roles and responsibilities;
- Processes;
- Practices.

7. ICT DELIVERY

7.1 Principles for ICT governance

The municipal-wide governance framework is based on principles as explained in MFMA, the international standard for IT governance, ISO/IEC 38500, King III report, COBIT and ITIL.

7.2 Table of ICT governance principles:

ICT GOVERNANCE PRINCIPLES
<u>Principle 1:</u> 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.

7.3 ICT governance oversight structure in the municipality

The need for the creation of this framework was (in addition to the basis factors) also informed by various investigations performed in the past. It was found that ICT is not effectively managed at various levels within the municipality as intended by applicable acts and regulations.

This framework should therefore create municipality-wide oversight structure to foster an integrated approach to the governance of ICT and ensure proper coordination between stakeholders. The oversight structure is:

- **Executive Management is responsible to foster an integrated approach to governance and ensure proper coordination.** The Executive Management is responsible for information and communication technologies in the municipality. The Executive Management may establish ICT norms and standards, make determinations and directives to improve the internal functioning of the municipality and to render effective services to the public.
- **ICT Management is responsible for the implementation and oversight of ICT governance in accordance with the ICT Governance Framework and implementation Guidelines.** The ICT Manager/CIO through the IT Steering Committee is the principal inter-departmental medium to coordinate, advise and facilitate the adoption and implementation of the governance of ICT.
- **The auditors conduct audits** and report on their findings to the relevant authorities.
- **Executive Management create a sustained enabling environment** for the implementation of ICT governance, and through monitoring/management ensure continuous improvement of ICT enabled service delivery and reporting.

7.4 Roadmap towards municipal governance

Initial Considerations

The roadmap to implement, control and govern ICT follows a generic approach of implementing ICT governance. It ensures that the focus is on municipal needs when improving control and governance. The roadmap encourages management commitment and involvement and follows good project management practices. The roadmap is a continuous improvement approach that is followed iteratively, building a sustainable ‘business as usual’ process over time.

Building sustainability entails:

- Integrating ICT governance with enterprise governance;
- Ensuring accountability for ICT throughout the municipality;
- Drafting and clearly communicating policies, standards and processes for ICT governance and control;
- Effecting cultural change (commitment at all levels in the enterprise, from the executive office to the 'shop floor');
- Driving a process and culture of continuous improvement; and
- Creating optimum monitoring and reporting structures.

In implementing ICT governance, the municipality will need to do so in a phased manner based on business priorities and ICT risks. The roadmap achieves this by prioritising the ICT goals and processes (including controls) based on the consideration of business goals and risks.

7.5 Critical success factors for business / ICT relationship

The following success factors are highlighted as necessary to ensure seamless implementation and integration in the delivery of sound ICT governance by the municipality:

- Good business acumen – Understand areas where ICT can add business value;
- ICT strategic sessions – Building a shared vision;
- Regular IT Steering Committee meetings;
- Cost-effective solutions at market related / optimal cost;
- Contingency planning – Formal business continuity planning as well as ICT disaster recovery planning;
- Effective contract management and performance management;
- Enhanced change management;
- Ongoing mitigation of strategic; and operational risks.

7.6 Organisational structure

A Municipal Manager is part of Executive Management of the municipality and also Accounting Officer of the municipality. S/he may delegate certain duties/tasks taking advise from CIO/ICT Manager, but remains accountable for:

- All transactions entered into by the municipality;
- Sound record management (Information Management).

Following the intentions of King III, it is suggested that:

- The municipal ICT function, be afforded the required strategic significance and be directly under the influence of the office of the Municipal Manager;
- The implementation of the governance of ICT is delegated from the office of the Municipal Manager to a Municipal IT Steering Committee made of the relevant executive / senior management (section 57 managers) as well as the Chief Information Officer and ICT Manager)

The following ICT Governance Organisational Structure will be adopted as per Figure 1:

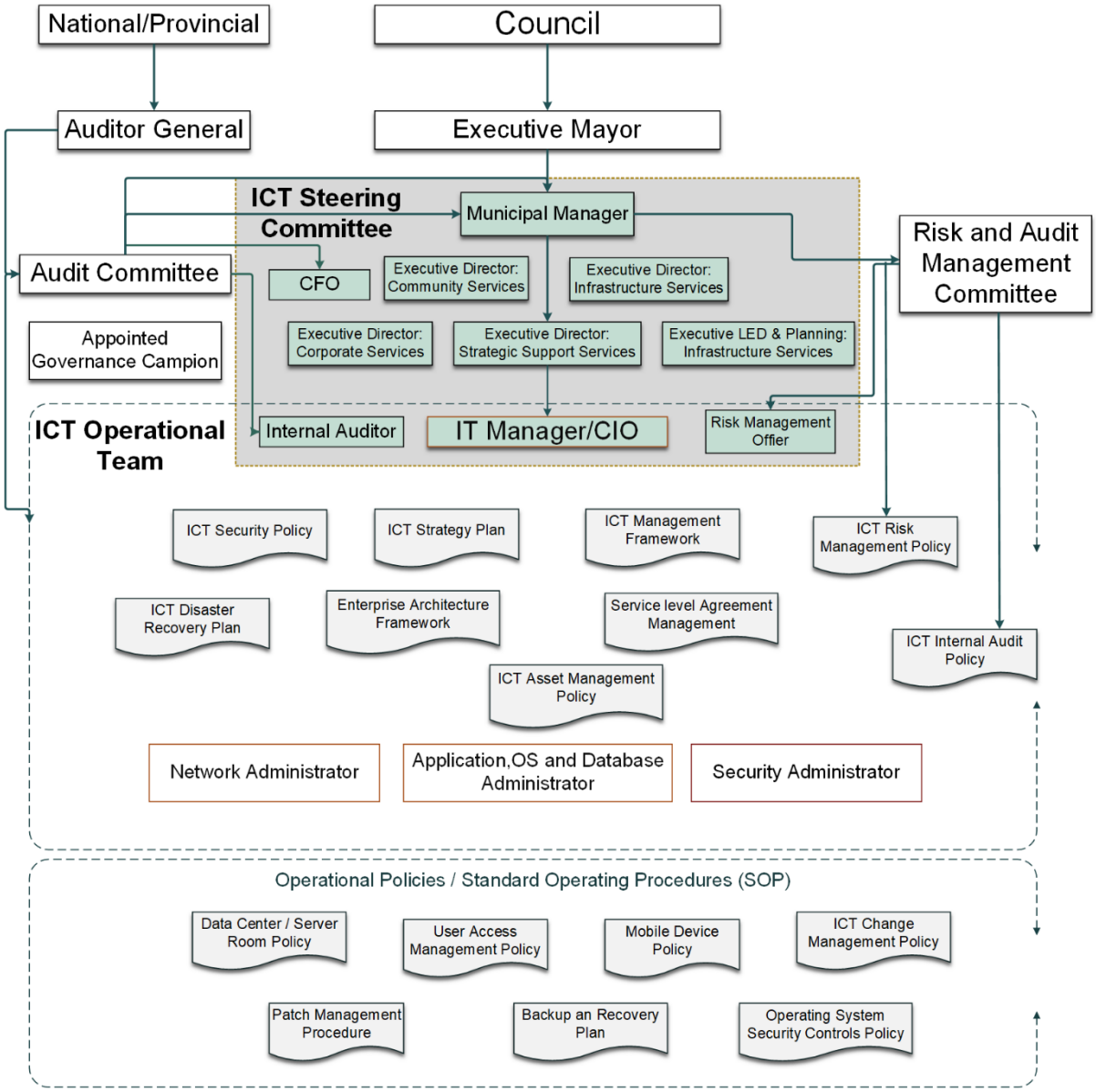

Figure 1 MCGICTP Organisational Structure

7.7 Municipal IT Steering Committee

The Municipal IT steering committee is to ensure that everyone in the municipality understands the link between business and ICT goals and accepts their responsibilities with respect to the supply and demand for ICT. The municipal IT steering committee will ensure that:

- The necessary ethical culture, structures (including outsourcing), strategies, policies, procedures, processes, mechanisms and controls regarding all aspects of ICT use (business and ICT) are clearly defined, implementing and enforced;
- ICT performances is assured through independent audit; and
- Intellectual property in information strategy is approved;
- Aspects relevant to ICT assets, privacy, security and personal information of employees are effectively managed.

7.8 ICT Manager / Chief Information Officer

The implementation and operation of governance is the responsibility of the Chief Information Officer/ ICT Manager who is expected to report to the IT steering committee and council about the effective and efficient management of ICT resources to facilitate the achievement of corporative objectives.

King III also requires the Chief Information Officer/ ICT Manager to define, maintain and validate the ICT value proposition, align ICT activities with environmental sustainability objectives, implement an ICT control framework and ensure all parties in the chain from supply to disposal of IT services and goods, apply good governance principles.

7.9 Implementation

Using COBIT 5 as a reference, the following steps will be used as a guideline for implementing an ICT Governance Framework. All steps listed below are to be administered by the Chief Information Officer/ ICT Manager.

1. **Raise awareness and obtain management commitment -** it is important to ensure that the background and drivers behind the initiative are understood clearly and that there is good support from top management.

2. **Define scope** - it is important for the implementation team to be knowledgeable about the business environment and to have an insight into influencing factors such as competition, business goals, service providers, legal and regulatory issues.

3. **Define risks** - it is important to know the municipality's risk profile, acceptance position and risk awareness so that an appropriate risk management attitude is taken.

4. **Define resources and deliverables** - The municipality must critically consider existence of assets and resources and establish how these can be leveraged.

5. **Plan programmes** - Based on the agreed- upon programme and resource requirements, the resources need to be acquired and allocated to the relevant programmes. Funding may be required to support the cost of these resources, and it may be necessary to acquire external consultants or experts.

6. **Access actual performance** - it is important to establish how well existing processes are managed and executed based on the process descriptions, policies, standards, procedures, technical specifications, etc., to determine whether they are likely to support business and ICT requirements.

7. **Define target for improvement** - based on the assessed current-state process maturity levels, an appropriate maturity level should be determined for each process.

8. **Analyse gaps and identify improvements** - after the current capacity of the processes has been determined and the target capacity planned, the gaps description between as- is and to-be should be evaluated and opportunities for improvement identified.

9. **Monitor implementation performance** - it is essential that the improvements can be monitored via ICT goals and ICT process description goals.

10. **Review program effectiveness** - determine whether the ICT governance programme delivered against expectations.

11. **Build sustainability** - build on the successes and lessons learned from the governance implementation project(s) to build and reinforce commitment amongst all ICT stakeholders for continuously improved governance of ICT.

12. **Identify new governance requirements** - using feedback and lessons learned, monitoring of performance and current understanding of business and ICT goals, the municipality should consider new governance requirements.

8. SHORT-TERM AND MEDIUM TO LONG TERM APPROACHES

Recommendations provided below are based on the premise that roles and responsibilities should be allocated to each activity. It is also crucial to the success of the deliverables that timelines (anticipated start and end dates) be allocated for each activity. The details will be incorporated in the ICT strategy and operational plans and are not detailed here-in.

To make this measurable, below is the RACI Model that is intended to be adopted for Implementation in Figure 2 below:

R A C I For Matjhabeng ICT Corporate Governance Framework	Executive Mayor	Municipal Manager	ICT Steering Committee	Finance	Strategic Support Services	Corporate Services	IT Manager/CIO	Network Administrator	APP, OS and Database Administrator	Security Administrator
ICT Strategy Plan	I	A	R	C	R	C	R	C	C	C
ICT Management Framework	I	A	I	C	R	R	R	I	I	I
ICT Portfolio management	I	A	I	C	R	R	R	I	I	I
ICT Risk Management	A	R	C	I	R	I	R	C	C	C
ICT Security Policy	A	R	R	I	R	I	R	R	R	R
Enterprise Architecture		A	R	C	R		R	C	C	C
Data Center / Server Room Policy		I	I				A	R	R	R
Operating System Security Controls Policy		R	C	C	I	I	A	R	R	R
ICT Asset Management		C	C	I	I		A	R	R	R
ICT Disaster Recovery Plan		A	C	C	R	C	R	R	R	R
Mobile Device Policy		I	C	C	I		A	R	R	R
Patch Management		I	C	C	R		A	R	R	R
Change Management		I	I	I	R		A	R	R	R
ICT Internal Audit Plan		A	R	C	R	C	R	C	C	C
Service level Agreement Management		A	R	C	R	C	R	R	R	R
Backup and Recovery Plan		A	I	I	R		R	C	C	C

Figure 2 RACI Mapping Model for Implementation

8.1 Short-Term

Control objectives and metrics will be assessed at operational level on an on-going basis, based on Standing Operating Procedures (SOP) and Policies where applicable. These include the following:

8.1.1 Security management

8.1.1.1 Dedicate responsibilities for information security to a dedicated information security officer, independent of the system administrator.

8.1.1.2 Design and implement ICT security policies and procedures for the administration of security measures over the network, operating system and application systems. These need to be enforced and updated on a regular basis.

8.1.1.3 Carry out ICT security awareness initiatives.

8.1.1.4 Manage and maintain ICT security at the highest appropriate organisational level.

8.1.1.5 Implement strong password controls to authenticate system access.

8.1.1.6 Correctly configure firewalls and routers within the network environment to ensure optimal protection against unauthorised access.

8.1.1.7 Implement and maintain path management processes to prevent exploitation of vulnerabilities.

8.1.1.8 Implement and maintain antivirus software across the organisation to protect information systems and technology from malware.

8.1.1.9 Ensure that system configurations detect security vulnerabilities and that incidents are monitored, reported and resolved on a regular basis.

8.1.1.10 Ensure that the activities within the system network, including database are tracked by using audit trails by someone independent of administration functions.

8.1.1.11 Firewall, Anti-Virus and Spyware solutions to make sure that your email, intranet and internet are protected from attack including:

- Monitored and Managed Firewall Services
- Managed Network –based intrusion Detection Services
- Managed Integrated Security Appliance Services
- Internet Vulnerability Assessment Services
- Managed Virus Protection Services

8.1.2 User access control

8.1.2.1 Formally documented and approved user account management standards and procedures.

8.1.2.2 Complete and get management approval for access request documentation for registering users, changing of access rights, passwords resets and termination of access rights.

8.1.2.3 Minimise the number of users with administrator privileges that can perform all functions pertaining to user account management.

8.1.2.4 Independently monitor activities of system administrators.

8.1.2.5 Periodically review employee access rights and privileges to ensure it is in line with their job responsibilities.

8.1.3 Change management

8.1.3.1 Establish and implement documented and approved change control policies and procedures

8.1.3.2 Ensure that administrators/users have the appropriate levels of access to the production environments with proper access control and audit mechanisms.

8.1.3.3 Where administrators/users have been granted access, ensure that access is monitored.

8.1.3.4 Complete and get management approval for change request documentation for all program changes.

8.1.3.5 Conduct user acceptance testing on all changes before migration to the production environment.

8.1.4 Data center management

8.1.4.1 Control changes to database management software

8.1.4.2 Restrict access to system software with access control software to personnel with corresponding job responsibilities.

8.1.4.3 Log and review installation of all system software to establish an audit trail.

8.1.4.4 Schedule hardware equipment changes /maintenance and testing to minimise the impact on operations and users.

8.1.5 Facilities and environmental controls

8.1.5.1 Control physical access to sensitive areas (e.g. computer room, operations, printing rooms, storage rooms, ups/generators, network rooms, tape library, offsite backup storage facility).

8.1.5.2 Periodically test environmental controls within data centres /computer rooms (e.g. water and smoke detectors, fire suppression system, fire extinguishers, air conditioning system).

8.1.6 ICT service continuity (Disaster Recovery, Backup and Restore)

8.1.6.1 Incorporate the ICT and disaster plans into organisational business continuity plan.

8.1.6.2 Distribute, update and test the ICT continuity plan and DRP and store at an offsite location.

8.1.6.3 Implement an ICT backup and retention strategy.

8.1.6.4 Perform backup procedures for data and programs according to above strategy.

8.1.6.5 Store backups in a secure offsite storage facility.

8.1.6.6 Implement physical access and environmental controls over offsite the storage facility.

8.1.7 ICT Infrastructure

8.1.7.1 This includes management of hardware such as Servers, Desktops, Notebooks and other ICT equipment,

8.1.7.2 Assess the warranty status of all machines

8.1.7.3 Develop an update plan as hardware comes out of vendor support or the end of serviceable life.

8.1.7.4 Document your current server hardware and create a report that shows where all your essential network services are currently located.

8.1.7.5 Develop a data map so that you can see where data is currently stored.

8.2 Medium to Long term

The following initiatives will be considered and performed:

8.2.1 Develop an ICT strategic Plan that supports business requirement

8.2.2 Prepare an organisation structure, indicating roles and responsibilities to ensure that ICT investments are aligned and delivered in accordance with enterprise strategies and objectives

8.2.3 Establishing an IT steering committee, chaired by the Municipal Manager and secretariat by the IT Manager with CFO and Director Strategic Support Services as permanent members and other senior management members attending by invitation. This will ensure that decisions taken in respect of ICT are taken in a coordinated manner.

8.2.4 Assess KPI's for ICT Governance on municipal ICT organisation level for compliancy.

8.2.5 Review ICT services performances periodically against targets.

8.2.6 Conduct regular ICT risk assessments to identify emerging risks.

8.2.7 Manage the relationship with suppliers through signed services level agreements (SLAs) to ensure the quality of outputs thereof.

8.2.8 Adopt a project management framework that defines the scope and boundaries of managing ICT projects.

8.3 ICT Governance Measurement

The measurement of ICT Governance performance in the municipality consists of a number of steps as defined below:

- **Define phase** – ICT Governance goals or Key Goal indicators (KGI's) need to be established at the top organisational level (Municipal Manager's Office). These goals are then cascaded down in the municipal ICT organisation. A KGI is a measure of "what" has to be accomplished.
- **Translation phase** – A cascading (breakdown) of the KGI into measurable (weighing factor) Key performance indicators (KPI's) and sources/processes cross the municipal divisions. A

KPI define and measure progress toward organisational goals. While KGI's focus on "what", the KPI's are concerned with "how"

- **Measurement phase** – Audits/ assessments (self-assessments) are conducted across the ICT environment on relevance of governance activities/ plans/ processes/ RACI within the business value chain. The level of accomplished ICT Governance process roll-out per business requirement is measured
- **Management phase** - From the audit/ assessment results, the cascaded KPI's/ KGI's are analysed for shortfalls and potential business risks coming from these (where not predefined) to enable corrective actions.
- **Opportunity phase** – Performance measures are then compared against the goals and the goals are checked for validity. Goals may be redefined because of business dynamics. Adjusted and the cycle starts over, periodically.

8.4 Support for governance

By establishing this framework, Matjhabeng realises that a support function will be a requirement to enable successful adoption and implementation. Apart from the usual support structures that are already in place, Matjhabeng will provide the following support structures:

1. **Skills development and awareness sessions: -** In line with the skills requirements that may be realised, Matjhabeng will provide educational workshops and awareness sessions on the various categories. These workshops and sessions will be made available on a regular basis.
2. **ICT Governance Assessments:** - A certain amount of ICT governance assessments are planned over the medium to long term to assist the municipality to measure ICT governance maturity levels.

8.5 Recommendations towards sound ICT governance

8.5.1 Executive Management should assume the responsibility for the governance of ICT and place it on Executive Management agenda.

8.5.2 Executive Management should ensure that an ICT charter and policies are established and implemented.

8.5.3 Executive Management should ensure promotion of an ethical ICT governance culture and awareness and of a common ICT language.

8.5.4 Executive Management should ensure that internal control framework is adopted and implemented.

8.5.5 Executive Management should receive independent assurance on the effectiveness of the ICT internal controls.

8.5.6 Executive Management should ensure that the ICT strategy is integrated with the municipality's strategic and business processes.

8.5.7 Executive Management should ensure that there is a process in place to identify and exploit opportunities to improve the performance and sustainability of the municipality through the use of ICT

8.5.8 Management should be responsible for the implementation of the structures, processes and mechanisms for the ICT governance framework.

8.5.9 Executive Management may appoint an IT Steering committee or similar function to assist with its governance of ICT.

8.5.10 The Chief Information Officer/ ICT Manager should be a suitably qualified and experienced person who should have access to, and interact regularly on strategic ICT matters with Executive Management and/ or appropriate committees.

8.5.11 Executive Management should oversee the value delivery of ICT and monitor the return on investment from significant ICT projects.

8.5.12 Executive Management should ensure that intellectual property contained in information systems is protected.

8.5.13 Executive Management should obtain independent assurance on the ICT governance and controls supporting outsourced ICT services.

8.5.14 Management should regularly demonstrate to Executive Management that the municipality has adequate business resilience arrangements in place for disaster recovery.

8.5.15 Executive Management should ensure that the municipality complies with ICT laws and that ICT related rules, codes and standards are considered.

8.5.16 Executive Management should ensure that there are systems in place for the management of information which should include information security, information management and information privacy.

8.5.17 Executive Management should ensure that all the personal information is treated by the municipality as an important business asset and is identified and secured accordingly.

8.5.18 Executive Management should ensure an Information Security Management System is developed and implemented.

8.5.19 Executive Management should approve the information security strategy and delegate and empower management to implement the strategy.

8.5.20 The risk committee/ or audit risk committee should ensure that ICT risks are adequately addressed.

8.5.21 The risk committee/ or audit and risk committee should obtain appropriate assurance that controls are in place and effective in addressing ICT risks.

8.5.22 The audit and risk committee should consider ICT as it relates to financial reporting and the going concern of the municipality.

8.5.23 The audit and risk committee should consider the use of technology to improve audit coverage and efficiency.

9. RISK MANAGEMENT

Risk Management is an integral part of the municipality's management processes and an essential function of corporate governance. The municipality's effectiveness is enhanced when risk management is part of the culture and is embedded in its values, practices and business processes.

Risk management focuses on the relationship between risk and its impact on achieving objectives. The alignment of risk management with the strategic planning processes facilitates closer interaction between the revision of plans and the reassessment of risks. It is most effective when an appropriate balance is realised between maximising the potential gains that are identified during the business planning process and minimising the potential losses of potential risk events.

All employees have a responsibility for managing risk in order to support the achievement of objectives.

Risk management and business continuity management need to be considered as a part of an integrated whole and, as such, business continuity management is considered a required outcome of the ICT governance process.

10. MAINTAINING THE ICT GOVERNANCE FRAMEWORK

It is the responsibility of the Chief Information Officer/ ICT Manager of the municipality to ensure that plans and procedures are in place to keep this framework up to date. If, whilst using the document, you find any information which is incorrect, missing or if you have a problem in understanding any part of this framework please inform the Chief Information Officer/ ICT Manager, so that it may be corrected. It is important that everyone understands his or her roles as described in this document.

Update versions of the framework are distributed to the authorised recipients from time to time.

11. TERMS AND DEFINITIONS

TERM	DEFINITION
AG	Auditor General
Accounting Officer	The Accounting Officer is the Municipal Manager who is the head of administration and Council and its committees on administrative matters such as policy issues, financial matters, organisational requirements and personnel matters.
BCM	Business Continuity Management
BITA	Business IT Alignment
BS 25999	Business standards for business continuity management (BCM)
Business Goals	Statements that describe the business will accomplish, or the business value a project will achieve – A clear vision of what you want to achieve and how.
Charter	A document that defines the purpose of the initiative, how it will work, and what expected outcomes are.
CFO	Chief Financial Officer
CIO	Chief Information Officer

TERM	DEFINITION
Cobit 5®	Control Objectives for Information and Related Technology, a globally recognised ICT governance framework, 2012 edition.
CoGTA	Department of Corporate Governance and Traditional Affairs
Control	A procedure or policy that provides a reasonable assurance that the Information Technology (IT) used by an organisation operates as intended.
Corporate Governance	The set of responsibilities and practices exercised by the Council and executive management with goals of providing strategic direction, ensuring that objectives are achieved, ascertaining that the risks are managed appropriately and verifying that the enterprise's resources are used responsibly.
CSS	Corporate Support Services
Deliverable	A term used in project management to describe a tangible or intangible object produced as a result of the project that is intended to be delivered to a customer.
DRP	Disaster Recovery Planning
EXCO	Executive Management
Executive 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 to a Constitutional Institution with a single office bearer, the incumbent of that office. According to section 11(1) of the Municipal Systems Act (Act No. 32 of 2000), the executive and legislative authority of a municipality is exercised by the council of the municipality.
Framework	A basic conceptual structure with items which supports a particular approach to a specific objective. E.g. CobiT 5 is an IT governance framework.
Governance of ICT	The effective and efficient management of IT resources to facilitate the achievement of company strategic objectives (King III: 2009). Is the responsibility of executives and board of directors, and consists of the leadership, organisational structures and processes

TERM	DEFINITION
	that ensure that the enterprise's IT sustains and extends the organisation's strategy and objectives (ITGI 2005).
ICT	Information and Communication Technology also referred as IT.
ISACA®	Information Systems Audit and Control Association
ISMS	Information Security Management System
IT Goals	Process that ensures that IT sustains and extends the organisation's strategy and objectives.
IT	Information Technology
IT Steering Committee	This is a management group composed of important decision makers from various departments within an organisation. This group is responsible for determining overall IT investment strategy, aligning IT solutions with business objectives.
ITIL	IT Infrastructure Library
ISO/IEC	International Standards Organisation (ISO) and the International Electro Technical Commission (IEC)
ISO/IEC 20000	International Standards for IT service management. It was developed in 2005 by ISO/IEC JTC1 SC7 and revised in 2011.
ISO/IEC 24762	International Standard – Security techniques – Guidelines for information and communications technology disaster recovery services.
ISO/IEC 27001/2	Part of ISO/IEC 27000 family of standards, is an Information Security Management System (ISMS) standard published in October 2005.
ISO/IEC 38500	International Standards Organization - The standard applies to the governance of management processes and information and communication services used by an organisation.
KGI	Key Goal Indicator. A KGI is a measure of "what" has to be accomplished.
King III	The King Code of Corporate Governance for South Africa 2009

TERM	DEFINITION
KPI	Key Performance Indicator. While KGI's focus on "what" the KPI's are concerned with "how".
LG SETA	Local Government Sector Education & Training Authority
LGTS	Local Government Turnaround Strategy
Metrics	A measure of an organisation's activities and performance
MFMA	Municipal Finance Management Act
MCGICTP	Matjhabeng Corporate Governance of ICT Policy
NT	National Treasury
Policy	A principle or rule to guide decisions and achieve rational outcome(s)
PAIA	Promotion of Access to Information Act
Process	Sequence of interdependent and linked procedures which at every stage consume one or more resources.
Procedure	A fixed, step by step sequence of activities or course of action (with definite start and end points) that must be followed in the same order.
RACI	Responsible, Accountable, Consulting and Informed mapping model
Responsible	Refers to the person who must ensure that activities are completed successfully.
Risk	The potential that a chosen action or activity (including the choice of inaction) will lead to a loss (undesirable outcome).
SABS	South African Bureau of Standards
SANS	System Administration, Network and Security Institute. SANS is by far the largest source for information security training and security certification n in the world.
SCOA	Standard Charter of Accounts
SSS	Strategic Support Services

TERM	DEFINITION
Strategy	The direction and scope of an organisation over the long-term which achieves advantage for the organisation through its configuration of resources.

12. APPROVAL

The signatories hereof, being duly authorised thereto, by their signature hereto authorise the implementation and/or adoption of this plan.

Municipal Manager, who hereby approves this ICT Governance Framework	Date
Executive Director: SSS, who hereby recommend and approves this ICT Governance Framework	Date
Acting ICT Manager: who hereby recommend this ICT Governance Framework	Date

Information Communication and Technology (ICT) Security Policy

Matjhabeng Local Municipality

(MLM)

Table of Contents

Document Information

Project Name:	ICT Security Policy		
Prepared By:	Matjhabeng ICT	**Document Version No:**	0.3
Title:	ICT Security Policy	**Document Version Date:**	08/05/2018
Reviewed By:		**Review Date:**	

Distribution List

Name	Date	Phone/Fax/Email

Document Version History

Version Number	Version Date	Revised By	Description	Filename
0.1	04/04/2018	Matjhabeng ICT	Document creation	ICT Security Policy
0.2	03/05/2018	Matjhabeng ICT	Inclusion of Email, internet usage, Remote access	ICT Security Policy
0/3	08/05/2018	Matjhabeng ICT	Revision of user access clauses	ICT INFORMATION SECURITY POLICY – Matjhabeng 1st DRAFT

1. INTRODUCTION

This document is of critical importance and every employee of Matjhabeng Local Municipality hereinafter refer to as “MLM” must ensure that he or she is familiar with its contents. It forms part of the conditions of all employees’ contracts of employment, and failure to adhere to the policies set out in this document may lead to disciplinary action and possible dismissal. When this policy is made applicable to non-MLM employees (for instance contract personnel), it shall form part of any contract between sub-parties and MLM.

The intention of this policy is to reduce risks that can be caused to the Municipality’s ICT systems, information and infrastructure. In addition, this policy defines the acceptable use of ICT resources by Officials and 3rd party service providers and breach or non-conformance is unacceptable.

2. SCOPE AND OBJECTIVES

2.1 This document (“the Policy”) sets out the policies and general guidelines of MLM, including its branches, divisions and subsidiary entities, (“the Municipality”) regarding access to and usage of the computer network, hardware and software, internet and electronic mail facilities and any other ICT related systems (“the Facilities”).

2.2 In this Policy document employee includes “User” and “User” means any person, including without limitation an employee, who has been granted the right to access and use the Facilities or any part thereof. Reference to “User” and “employee” may be made interchangeably and same must be interpreted in the context in which it is used.

2.3 Without limiting its scope, the Policy is intended to:

2.3.1 Ensure business continuity and protect the Municipality and its employees from potential liabilities which could result from inappropriate and unprofessional use of the Facilities.

2.3.2 Safeguard confidential and proprietary information of the Municipality and its customers which may be stored on the Facilities from loss or unauthorised access, use or disclosure;

2.3.3 Protect the Facilities from being damaged or disabled as a result of access by unauthorised persons or by viruses, malware, trojan horses, worms, disabling programmes and/or other destructive code;

2.3.4 Regulate the manner and circumstances in which employees of the Municipality are entitled to make use of the Facilities;

2.3.5 Ensure that the reputation of the Municipality is not harmed or otherwise infringed by inappropriate or unprofessional use of the Facilities.

2.4 This Policy is intended to be illustrative of the range of acceptable and unacceptable uses of the Facilities and is not necessarily exhaustive. Questions about specific uses relating to security issues are not enumerated in this Policy; reports of specific unacceptable uses should be directed to the ICT Security Administrator.

2.5 This Policy may be amended or supplemented from time to time

2.6 Specific categories of employees may be required to adhere to additional rules regarding use of the Facilities. In these circumstances, such additional rules shall be communicated to those employees in writing and shall be read with and form part of this Policy insofar as those employees are concerned.

2.7 To provide suitable coverage of International Standards ISO/IEC 17799:2005 and related information security best practices.

3. APPICABILITY

This policy shall apply to all persons as set out in paragraphs 1, 2.1 and 2.2

4. RESPONSIBILITIES

The ICT Manager is responsible for regular updates and audits of the Information Technology Policy. He/She shall also ensure the enforcement of the Policy throughout the Municipality. All enquiries regarding the Policy must be directed to him/her. He/she will be assisted by the ICT Security Administrator who is responsible for the tasks indicated in the Policy. All Users of the Facilities must report any transgressions of the Policy to the ICT Security Administrator and/or ICT Manager.

5. POLICY DESCRIPTION

5.1 GENERAL

5.1.1 All employees using the Facilities are required to:

5.1.1.1 Respect the privacy of others; for example, without limiting the generality of the a foregoing, Users shall not intentionally seek information on, obtain copies of, or modify files or data, belonging to other Users, unless explicit permission to do so has been obtained from that User;

5.1.1.2 Respect the legal protection provided to programmes and data by copyright and licence;

5.1.1.3 respect the integrity of computer systems; for example, without limiting the generality of a foregoing, Users shall not use or develop programmes that harass other users or infiltrate a computer or computing system and/or

damage or alter the software components of a computer or computing system.

5.1.2 No User of the Facilities may:

5.1.2.1 Re-allocate any hardware or software forming part of the Facilities without the prior approval of the Municipality's ICT Security Administrator.

5.1.2.2 Connect any hardware or install any software including personal hardware or software without the prior inspection and written approval of the Municipality's ICT Security Administrator.

5.1.3 Nothing that is generated on any part of the Facilities, whether personal or otherwise, shall in any way be private to any User, nor shall the User have any rights whatsoever over any material generated by or stored on, any part of the Facilities, all of which shall be the property of the Municipality.

5.1.4 Limited personal use of the Facilities shall be tolerated by the Municipality provided that personal usage:

5.1.4.1 Does not interfere with or impact upon the User's time and work responsibilities towards the Municipality;

5.1.4.2 Does not in any material way impact of the Municipality's bandwidth or electronic storage space;

5.1.4.3 Always subject to this Policy.

5.1.5 The Facilities may not be used for:

5.1.5.1 Subject to clause 5.1.4, any activity other than Municipality business, such as, without limitation, private purposes such as marketing or business transactions;

5.1.5.2 Solicitation for religious and/or political or similar causes;

5.1.5.3 Unauthorised not-for-profit activities;

5.1.5.4 Private advertising of products or services;

5.1.5.5 Any activities meant to foster personal gain by an employee;

5.1.5.6 Revealing or publishing information that is of a proprietary or confidential nature to Municipality or any third party.

5.2 IDENTITY AND ACCESS

5.2.1 The Municipality has the right to approve or reject any application by any person for access to its Facilities

5.2.2 The access permission of any User may be terminated or limited at any time without prior notice.

5.2.3 Subject to clause 5.1.4, access to the Facilities shall only be granted for the purposes of conducting the business of the Municipality and all Users are required to limit personal use

of the Facilities to that which is appropriate and/or incidental to the User's job responsibilities.

5.2.4 Save as provided for in 5.1.4, all Users shall not use the Facilities for activities unrelated to the general objectives of MLM, unrelated to the employee's job responsibilities or for any illegal purpose.

5.2.5 Employees shall arrange for a substitute, who shall be an employee, to monitor incoming electronic mails whilst the employee is on leave.

5.2.6 Anonymous identities are not allowed, and are implicitly prohibited when accessing confidential information under any circumstance.

5.2.7 Information users will be given the minimum level of access to systems and information that their duties require.

5.2.8 Human Resources Management division must report change of an employee employment status or role to ICT Department for revocation of access.

5.2.9 Passwords, pass-phrases, and private keys (physical and private digital) must be protected, and may not be shared.

5.2.10 The **"ICT User and Access Management Policy"** that is available to all users will be binding and will be used for enforcement of users' access. This document is available on the Intranet on Network Share location: shared drive/OneDrive

5.3 THIRD PARTY AND REMOTE ACCESS

5.3.1 The Municipality has the right to approve or reject any application by any person for remote access including, but not limited to Remote Desktop applications and services along with the Municipality's VPN.

5.3.2 The remote access permission of any User may be terminated or limited at any time without prior notice.

5.3.3 Remote Access to the Municipality network shall only be via specific TCP/IP ports and or services authorised by the ICT Security Administrator. The use of any other ports and/or services is not permitted.

5.4 SECURITY

5.4.1 No User is allowed to use or work on in any way, a computer other than the computer allocated to that specific user by ICT, hence no private computers may be connected to the network.

5.4.2 All Users must safeguard their user-id and/or passwords and these are not to be shared with any other person without authorisation. Should a User become aware that their password has been revealed to a third party, the User must immediately contact the ICT Security Administrator/helpdesk in order to disable the account and/or change the

password. All Users shall report any attempted unauthorised use of their password of which they become aware.

5.4.3 Passwords are not to be stored in an accessible paper based format or in any other manner easily accessible to other Users and no User may work on or in any way abuse the Facilities through the utilisation of another User's password, account or user-id.

5.4.4 Users shall be held personally liable for any misconduct, loss or damage resulting from the use of the Facilities by another person using their password, account or user-id unless the User can prove that the unauthorised person's access to their password, account or user-id did not come about through any wilfulness or neglect on the part of the User.

5.4.5 Passwords will be changed as often as required, but no less frequently than once every thirty (30) days.

5.4.6 Users will be allowed three (3) attempts within which to enter their passwords when logging in. If the third attempt fails, the User shall be prevented from gaining access to the Facilities and will have to contact the ICT Security Administrator to gain access.

5.4.7 All Users must immediately notify the ICT Security Administrator of any security breaches and are not to advise, or demonstrate the problem to, others.

5.4.8 All computers will be set to hibernate/sleep within 3 minutes if not attended and will require users to login.

5.4.9 No User shall, without authorisation, distribute or disseminate the Municipality's data and information or client's data and information belonging to customers of the Municipality.

5.4.10 No User may import non-text files or unknown messages onto the Facilities without having scanned them for viruses. All attachments must be treated with utmost caution to prevent the import of malicious software into the network of the Municipality.

5.4.11 All portable storage media, including but not limited to USB, portable HDD and tapes shall be adequately secured when not in use, by, for example, being locked away and should be in an environment that is free from hazards such as heat, direct sunlight and magnetic fields.

5.4.12 No User may allow another person who is not an employee of the Municipality to have access to any Facilities belonging to the Municipality unless that person has been authorised to have access by the ICT Security Administrator.

5.4.13 No User may remove any computer hardware including without limitation, portable computer hardware belonging to the Municipality from its premises without the prior written consent of the Municipality.

5.4.14 In relation to laptop, notebook or other portable computers belonging to the Municipality, the User of any such hardware must from time to time show that:

5.4.13.1 The hardware is present at the Municipality's premises at all times except when it is being used outside of the Municipality's premises for the Municipality's business;

5.4.13.2 The User has taken all reasonable steps to safeguard the hardware in their

possession;

5.4.13.3 The hardware is adequately secured at all times, for example, by being locked away when not in use or being locked to a fixed securing cable.

5.4.13.4 Any hardware (e.g. laptops, tablets, smartphones, storage) not being property of the Municipality shall not be connected to the network of the Municipality without prior written consent of the ICT Security Administrator. The access to the network of the Municipality, if granted, will only be temporary and given on a case by case base.

5.5 INFORMATION HANDLING

5.5.1 Unauthorised disclosure of sensitive information is prohibited.

5.5.2 Unauthorised tampering or alteration of sensitive information is prohibited.

5.5.3 Unauthorised destruction or disposal of sensitive information is prohibited.

5.5.4 Laws and policies governing information retention must be complied with.

5.5.5 When confidential information is being transported or stored, it must be protected from unauthorised disclosure, modification, or destruction.

5.5.6 When possible, confidential information must be protected with sufficient publicly vetted encryption algorithms while in transit and at rest.

5.5.7 If encryption is not possible then the appropriate compensating controls must be considered and implemented.

5.5.8 Before access is granted to confidential information, a signed non-disclosure agreement must be on file for that individual or organisation.

5.5.9 When appropriate, criminal and reputational background checks must be conducted.

5.5.10 Confidential information being transported to or stored with a third party outside of the Municipality network or physical premise must be approved by the Information Owner.

5.5.11 Confidential information, both digital and physical, must be disposed properly to prevent unauthorised disclosure.

5.6 CONFIDENTIALITY

5.6.1 The Municipality retains all rights of whatsoever nature in and to any material created on its Facilities, including but not limited to all data processed and/or extracted within the Municipal ICT network, and no User shall acquire any rights of whatsoever nature in and to the materials so created, which shall at all times be the exclusive property of the Municipality.

5.6.2 The Facilities have no capability to enable the sending or receiving of private or personal, confidential electronic communications. The ICT Security Administrator has access to all electronic mail and User access requests and will monitor messages as necessary to

ensure efficient performance and appropriate use. Messages relating to, or in support of, illegal or unauthorised activities will be reported to the appropriate authorities.

5.6.3 Any Municipality information related to strategy, planning, finance, rating, pricing, employee remuneration or performance details, statutory records, minutes of meetings, correspondence, internal memoranda, research or any other information relating to the Municipality not in the public domain, or intended for general or public use, is to be treated as confidential by all Users.

5.6.4 All Users are permitted to view public folder contents except where access has been restricted and/or denied.

5.6.5 No users at anytime may access other users' information using any access form/method without permission.

5.6.6 No administrator's passwords may be shared with end users in any case. ICT professionals failing abide to this will face disciplinary actions which may lead to dismissal.

5.6.7 No private/personal laptops may be operated in ICT by ICT staff members.

5.6.8 **Sensitive information:** Information in this category may not be distributed without consideration of its sensitive nature further elaborated as follows:

5.6.5.1 Private information is personal information, including personal intellectual property, which is accessible only by its owner and those to whom the owner directly entrusts it, except under exceptional circumstances. Examples: Intellectual property, email;

5.6.5.2 Confidential information is Municipality information normally handled in the same manner as private information, but may be accessed by other authorised employees under limited additional circumstances, Examples: ID number, date of birth, medical records, education record, financial record;

5.6.5.3 Internal information is Municipality information that is intended for distribution within the Municipality.

5.6.9 **Public Information:** Information in this category is distributed without restriction. Examples: Marketing materials, Municipality website

5.6.10 **Top Secret:** shall be applied to information, the unauthorised disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Example: Compromise of complex cryptologic and communications intelligence systems.

5.6.11 **Secret:** shall be applied to information, the unauthorised disclosure of which reasonably could be expected to cause serious damage to the national security. Example: Revelation of significant intelligence operations

5.7 INTERNET USAGE

5.7.1 No User shall:

5.7.1.1 Upload or download commercial software in violation of its copyright and no software may be uploaded to websites without the authorisation;

5.7.1.2 Download any software or electronic files without reasonable virus protection measures in place and all Users are expected to adhere to the virus protection procedures of the Municipality,

5.7.2 Intentionally introduce a virus into the Facilities. Any User who suspects that his or her hardware has been infected by a virus, shall immediately unplug his/her network cable and contact the IT Security Administrator,

5.7.3 Intentionally interfere with the normal operation of any internet gateway.

5.7.4 The Internet shall not be used by Users for representing personal opinions as those of the Municipality.

5.7.5 No personal communications may be posted to any worldwide website or news group without the author's consent and no anonymous messages may be posted using the Facilities.

5.7.6 Subject to clause 5.1.4, the Internet shall only be used for the Municipality's business purposes.

5.7.7 No website shall be developed or implemented using the Facilities without the authorisation of the Municipal Manager.

5.7.8 Internet Explorer and Google Chrome are the only internet browsing software that may be utilised.

5.7.9 The User shall be responsible for the proper use of the Internet.

5.7.10 A connection to the Internet may not be established if the User does not intend to make use of it and all connections must be terminated before leaving the computer work station. The duration of an internet connection is limited to a maximum of 4 hours, unless otherwise strictly required for the Municipality's business purposes.

5.7.11 Users may not send confidential information via the internet without appropriate encryption controls as it is not a secure medium.

5.7.12 No information may be published about the Municipality via the internet without the authorisation of the Municipal Manager.

5.7.13 No links from the Municipality's website may be established without the prior authorisation of the Municipal Manager. The Facilities may not be used to transmit threatening, excessive, obscene or harassing materials or correspondence.

5.7.14 The Facilities may not be used for the viewing of websites containing obscene, pornographic, sexist, racist, profane or unlawful content.

5.7.15 The Facilities may not be used for the playing of online or any other types of games.

5.7.16 The ICT Department will use Network devices that will control and enforce the internet usage accordingly.

5.8 ELECTRONIC MAIL (E-MAIL)

5.8.1 Subject to clause 5.1.4, the Municipality's electronic mail Facility is to be used for both internal communication and communication with external third parties for the business purposes of the Municipality only.

5.8.2 Microsoft Outlook and Microsoft Office 365 are the standard software used for sending and receiving electronic mail and no other software may be used for this purpose.

5.8.3 When sending messages and communications via electronic mail, all Users must ensure that:

5.8.3.1 Paper based copies of electronic mails are printed out, signed by the initiator and retained for record keeping purposes as if they were a telefax

5.8.3.2 A satisfactory confirmation of receipt is obtained for important messages. This may mean contacting the recipient in the case of important messages;

5.8.3.3 All messages and communications contain the Municipality's name, together with that of the sender of the message, as well as any standard confidentiality caution wording stipulated by the ICT Security Administrator from time to time and that all computers which Users have access to are configured in such a way that this occurs automatically when any electronic communication is sent;

5.8.3.4 No messages are threatening, excessive, obscene, harassing or illegal and no abusive, sexist, racist or otherwise objectionable language may be used in any electronic mail messages;

5.8.3.5 No chain letters may be sent, messages may not be broadcast and no use may be made of the electronic mail system which would cause congestion of the network or otherwise interfere with the work of others;

5.8.3.6 No messages may be sent by electronic mail without appropriate encryption controls which could cause damage or loss if the contents were revealed to anyone other than the intended recipient;

5.8.3.7 Personal electronic mail sent by Users should be clearly labelled as such;

5.8.3.8 The Municipality's electronic mail Facility may not be used for unauthorised distribution or dissemination of the Municipality's confidential and proprietary information, or its customer's data and information.

6. ASSESSMENT AND COMPLIANCE

6.1 Risk assessments must be regularly conducted to reveal security posture, and to identify vulnerabilities and weaknesses in software, infrastructure, policy, procedure and practices.

6.2 Users will be required upon logging into the Matjhabeng ICT network Acknowledge and Accept the Policy.

6.3 Ongoing training and awareness sessions for ICT Security are available and the onus is upon all users to familiarize themselves with this policy.

6.4 Violation of this policy, may lead to restriction of access to the ICT facilities or disciplinary action.

6.5 Any damage, security breach or loss of information which can be deemed to have been caused by negligence or intention on the part of the user or any identified individual will be the responsibility of that user or that individual. The penalty, thereof, will be determined by the Municipality disciplinary process.

6.6 The Matjhabeng ICT Department will use enforced devices including but not limited to Firewalls, IPS/IDS, Vulnerability Systems and/or other perimeter device security systems to ensure compliance to the Policy.

6.7 The Municipality may use any legislation relevant to the usage or protection of Information Systems (or information), in prosecuting the person who has violated this policy.

6.8 Logs and Access of employees recorded by ICT systems will be deemed as sufficiently evidence for action against employees that are found in breach of this policy, such systems are as follows:

6.2.1 Logs from Domain Controllers, DHCP Servers and/or Network Access Servers

6.2.2 Operating System administration access logs including source IP address, time of activity and changes made.

6.2.3 Radius and/or Tacacs audit trail logs

6.2.4 Applications and 3rd Party service provider access logs.

6.2.5 ICT Reporting and Management systems.

6.9 Employees must participate in information security awareness that will be provided by the ICT Department from time to time and the obligation is on employees to acknowledge this policy

6.10 Controls shall be in place to ensure compliance with legal, legislative, regulatory or contractual obligations and any other security requirements.

7. TERMS AND ABBREVIATIONS

MLM	- Matjhabeng Local Municipality
ICT	- Information, Communications and Technology
Virus	- A computer virus is a type of malicious software program that, when executed, replicates itself by modifying other computer programs and inserting its own code.
Malware	- short for malicious software, is an umbrella term used to refer to a variety of forms of hostile or intrusive software.
Worms	- is a standalone malware computer program that replicates itself in order to spread to other computers
ISO/IEC 17799:2005	- establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization.
VPN	- Virtual Private Network
TCP/IP	- Transmission Control Protocol / Internet Protocol

USB	- Universal Serial Bus
HDD	- Hard Disk Drive
DHCP	- Dynamic Host Configuration Protocol
Radius	- Remote Authentication Dial-in User Service
Tacacs	- Terminal Access Controller Access Control Systems
Firewall	- Network Security device to block and limit access to applications
IPS/IDS	- Intrusion Prevention System / Intrusion Detection Sytem

8. APPROVALS

The signatories hereof, being duly authorised thereto, by their signature hereto authorise the implementation and/or adoption of this policy.

Municipal Manager, who hereby approves this ICT Security Policy	Date
Executive Director: SSS, who hereby recommends and approves this ICT Security Policy	Date
ICT Manager: who hereby recommends this ICT Security Policy	Date

Information Communication and Technology (ICT) Antivirus Policy
Matjhabeng Local Municipality
(MLM)

Table of Contents

Document Information

Project Name:	ICT Antivirus Policy		
Prepared By:	Matjhabeng ICT	**Document Version No:**	0.1
Title:	ICT Antivirus Policy	**Document Version Date:**	12/09/2018
Reviewed By:		**Review Date:**	

Distribution List

Name	Date	Phone/Fax/Email

Document Version History

Version Number	Version Date	Revised By	Description	Filename
0.1	11/09/2018	Matjhabeng ICT	Virus Management	ICT ANTIVIRUS POLICY – Matjhabeng 1st DRAFT

Introduction

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, CDs and Memory sticks. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to Matjhabeng Municipality in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of Matjhabeng Municipality is to provide a computing network that is virus- free. The purpose of this policy is to provide instructions on measures that must be taken by Matjhabeng Municipality employees to help achieve effective virus detection and prevention.

Scope

This policy applies to all computers that are connected to the Matjhabeng Municipality network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both Municipal-owned computers and personally-owned computers attached to the Matjhabeng Municipality network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, servers and cloud storage connected to the network.

Policy description

1. Currently, Matjhabeng Municipality has a Microsoft Endpoint Protection Antivirus licensed through System Centre. Licensed copies of Microsoft Endpoint Protection Antivirus can be obtained within a domain automatically when a user connect a device to the Municipal network. The most current available version of the anti-virus software package will be taken as the default standard. Where for any reason the Microsoft Endpoint Protection Antivirus is not available, an open source antivirus will be provided temporarily.

2. All computers attached to the Matjhabeng Municipality network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

3. Any activities with the intention to create and/or distribute malicious programs onto the Matjhabeng Municipality network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.

4. If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the ICT Section immediately at 3422 / 3136 / 3457. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.

5. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the ICT Section.

6. Any virus-infected computer will be removed from the network until it is verified as virus-free.

Rules for Virus Prevention

1. Always run the standard anti-virus software provided by Matjhabeng Municipality.

2. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

3. Never open any files or macros attached to an e-mail from a known source (even a co-worker) if you were not expecting a specific attachment from that source.

4. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

5. Files with the following filename extensions are blocked by the e-mail system: .exe, .zip, related. While sending/receiving business-critical files with banned extensions, such as use of a file compression utility please be advised that most of those extensions are also blocked on the email services, so even if you have compressed your own file into a Zip file it may not reach its destination as the email service may block it.

6. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

7. Avoid direct disk sharing with read/write access. Always scan a memory stick for viruses before using it.

8. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

9. Back up critical data and systems configurations on a regular basis and store backups in a safe place.

10. Regularly update virus protection on personally-owned home computers that are used for business purposes. This includes installing recommended security patches for the operating system and other applications that are in use.

ICT Responsibilities

The following activities are the responsibility of the Matjhabeng Municipality's ICT Section:

11. The ICT Section is responsible for maintaining and updating this Anti-Virus Policy. Copies of this policy will be posted to the workstation directly from the domain distribution server. System Administrator needs to check antivirus updates regularly for updated information or definitions.

12. The ICT Section will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use.

13. The ICT Section will apply any updates to the services it provides that are required to defend against threats from viruses.

14. The ICT Section will install anti-virus software on all Matjhabeng Municipality owned and installed desktop workstations, laptops, and servers.

15. The ICT Section will assist employees in installing anti-virus software according to standards on personally-owned computers that will be used for business purposes.

16. The ICT Section will only advise or and provide open source anti-virus software in these cases.
17. The ICT Section will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the ICT Section may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

18. The ICT Section will perform regular anti-virus sweeps of .exe, macros and related files.

19. The ICT Section will attempt to notify users of Matjhabeng Municipality systems of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

Department and Individual Responsibilities

The following activities are the responsibility of Matjhabeng Municipality departments and employees:

20. Departments must ensure that all departmentally-managed computers have virus protection that is in keeping with the standards set out in this policy.

21. Departments that allow employees to use personally-owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.

22. All employees are responsible for taking reasonable measures to protect against virus infection.

23. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the Matjhabeng Municipality network without the express consent of the ICT Section.

Policy enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action.

Declaration of understanding

This policy will be made available to access of every employee in the municipality to read, understand, and agree to adhere to this document as Matjhabeng Municipality's Anti-Virus Policy.

Approvals

The signatories hereof, being duly authorised thereto, by their signature hereto authorise the implementation and/or adoption of this policy.

Municipal Manager, who hereby approves this ICT Security Policy	Date
Executive Director: SSS, who hereby recommends and approves this ICT Security Policy	Date
Acting ICT Manager: who hereby recommends this ICT Security Policy	Date

Information Communication and Technology (ICT) Strategic Plan

Matjhabeng Local Municipality

Table of Contents

Document Information

Project Name:	ICT Strategic Plan		
Prepared By:	Matjhabeng ICT	**Document Version No:**	0.5
Title:	ICT Strategic Plan	**Document Version Date:**	08/05/2018
Reviewed By:		**Review Date:**	

Distribution List

Name	Date	Phone/Fax/Email

Document Version History

Version Number	Version Date	Revised By	Description	Filename
0.1	04/04/2018	Matjhabeng ICT	Document creation	ICT Strategic Plan
0.2	18/04/2018	Matjhabeng ICT	Insertion of AS-IS, Strategic Drivers, SWOT Analysis and Implementation Plan in parts	ICT Strategic Plan
0.3	24/04/2018	Matjhabeng ICT	Update of SWOT, inclusion of Overall strategic diagram	ICT Strategic Plan
0.4	04/05/2018	Matjhabeng ICT	Document update	ICT Strategic Plan
0.5	07/04/2018	Matjhabeng ICT	Org Structure and Implementation Plan inclusion	ICT Strategic Plan 1st DRAFT

1. INTRODUCTION

The Matjhabeng Local Municipality ICT Department has reviewed the existing policies and plans that are available along with feedback from the AG report has decided to formulate an ICT Strategic Plan. The purpose of this document is to ensure that the alignment of ICT is closer to the realization of the IDP drivers along with the expectation for improved service delivery.

2. APPROACH

The approach that has been adopted is based on areas that ICT is responsible and accountable for whilst appreciating the practicality of having an all-encompassing ICT Strategic Plan executable with the relevant frameworks and mandates within Matjhabeng Local Municipality.

These drivers were considered as follows:

2.1 INPUTS FROM THE IDP

Back to Basic

Municipalities are mandated to provide effective and efficient quality services to the residents and stakeholders in the city. Whilst tremendous progress has been made, there are areas that would require additional effort to ensure that acceptable service delivery standards are reached. To assist municipalities to achieve acceptable levels of services, CoGTA has implemented a Back to Basics program which all municipalities have to subscribe to. The program is directed at service the people and built on five pillars, as listed below.

The Back To Basics program identifies 4 priority areas of intervention as immediate priorities for transformation, to encourage all municipalities to be functional centers of good governance.

Priority 1: Get all municipalities out of a dysfunctional state and at the very least able to perform the basic functions of local government.
Priority 2: Support municipalities that are at a minimum basic level of performance to progress to a higher path.
Priority 3: Supporting and incentivize municipalities that are performing well to remain there.
Priority 4: Targeted and vigorous response to corruption and fraud, and a zero tolerance approach to ensure that these practices are rooted out.

The institutionalization of the Back to Basics would be via a performance management system to recognize and reward good governance based on performance measures, such as:

- Putting people first
- Delivering basic services

- Good Governance
- Sound financial management
- Building Capacity

All three spheres of government have an important role to play in ensuring well-functioning municipalities. Back to basics is the framework for government collective action.

ICT based objectives that are inputs from the IDP are summarized as per below:

- Build Multi-purpose centre
- Call Centre
- Decentralize Municipal offices
- Full operation of Municipal offices in townships
- Free Wi-Fi
- Job creation projects
- Use 5% of budget to attract investors
- Maintain and re-vitalize CBD

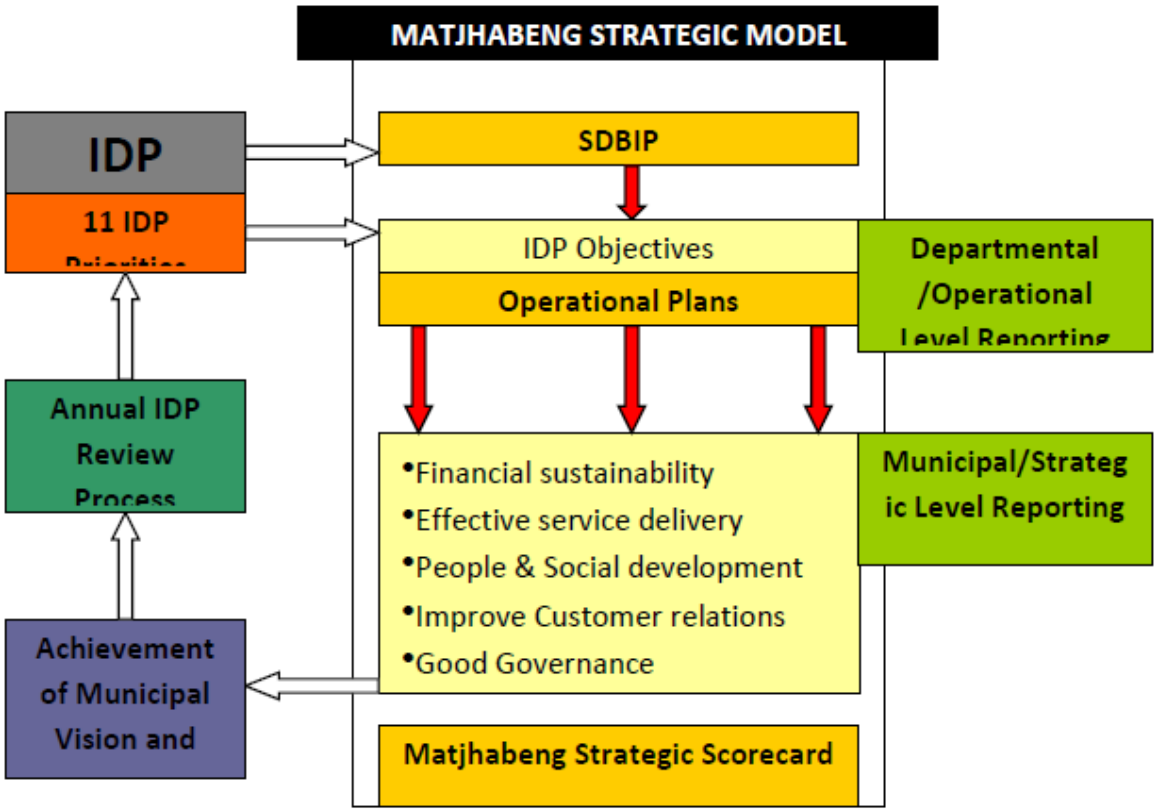

Figure 1: Matjhabeng strategic model from IDP

2.2 HOLISTIC APPROACH FOR INCLUSIVE ICT STRATEGIC PLANNING

The Matjhabeng ICT Strategic Plan is driven in an all-inclusive manner, taking into consideration the business drivers both internal and external, the effectiveness and readiness of the existing Operating Systems (OS), Databases, Backup solutions, server, network, cabling and physical environment conditions in order to be geared towards up to date technology platforms that are aligned to stakeholders' needs for a long-term period.

This is succinctly represented as follows:

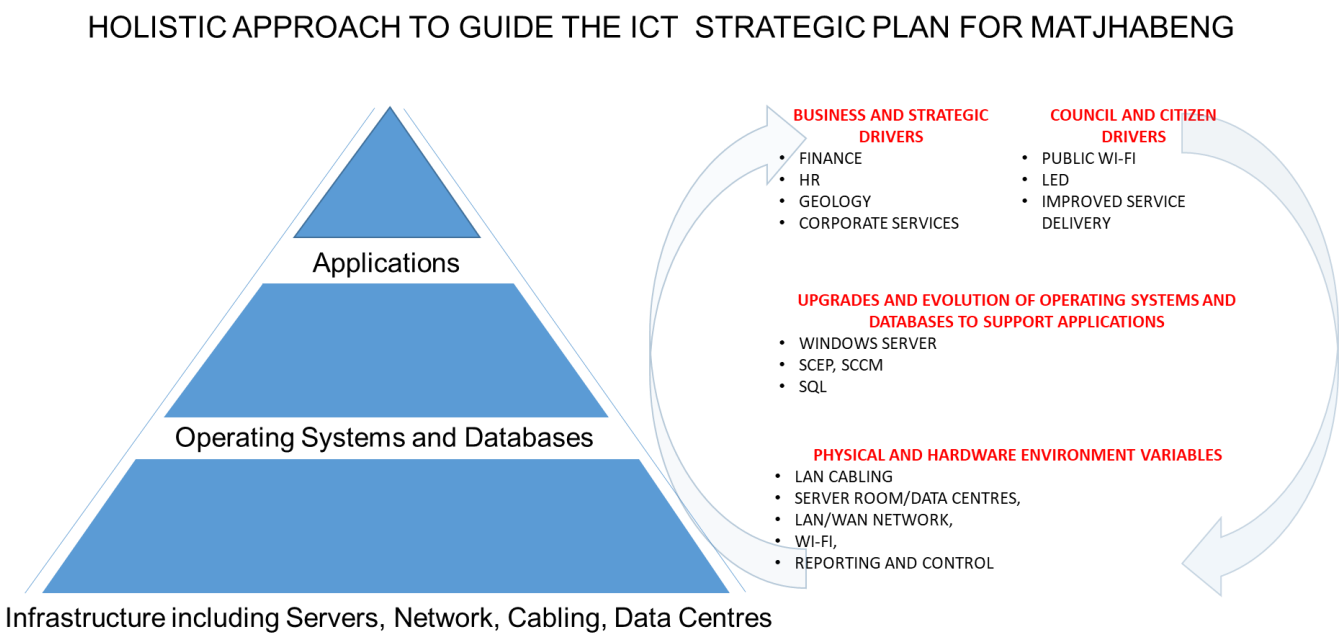

Figure 2: Strategic plan drivers

3. AS-IS ASSESSMENT SUMMARY

The current ICT Environment at Matjhabeng is composed of the following environments:

3.1 ICT ORGANIZATIONAL STRUCTURE

3.2 Head Office in Welkom

3.2.1 This is the main campus that has 4 separate buildings which are the Civic Centre Main Building, Reinet Building, Public Safety & Engineering Building and Finance Building with the main server room located at Civic Centre Building where all sites including Regional and Satellite sites connect to.

3.2.2 Overview of users and infrastructure supported by ICT:

Description	Quantity
USERS	Approx. 500
LAN SWITCHES	28
FIREWALLS	1
SERVERS	20
PATCH ROOMS	23
SERVER ROOMS (DATA CENTRE)	1
KEY APPLICATIONS	CashDrawer, Syntell, Solar, PayDay, Exchance, Network Share Drives, Paperless Agenda; Anti-virus; Internet

TABLE 1: ICT Users and Infrastructure Overview – Head Office Welkom Campus

3.3 Regional Sites/Units

Total of 5 x Sites/Units which are Allanridge, Ventersburg, Hennenman, Virginia and Odendaalsrus.

Description	Quantity
USERS	100
LAN SWITCHES	11
PATCH ROOMS / RACKS	9
KEY APPLICATIONS USED	PayDay, Cash Drawer, Solar, Email, Internet , Anti-virus, Paperless Agenda

TABLE 2: ICT Users and Infrastructure Overview – Regional Sites

3.4 Satellite offices listed below:

List of Satellite Sites:

Description	Quantity
USERS	94
LAN SWITCHES	13
PATCH ROOMS / RACKS	7
KEY APPLICATIONS USED	PayDay, Cash Drawer, Solar, Email, Internet, Paperless Agenda NOTE: Waste Management users are Testing an Application that is not hosted on any server but is key for testing purposes currently.

TABLE 3: ICT Users and Infrastructure Overview – Satellite Sites

3.5 Network Connectivity diagram:

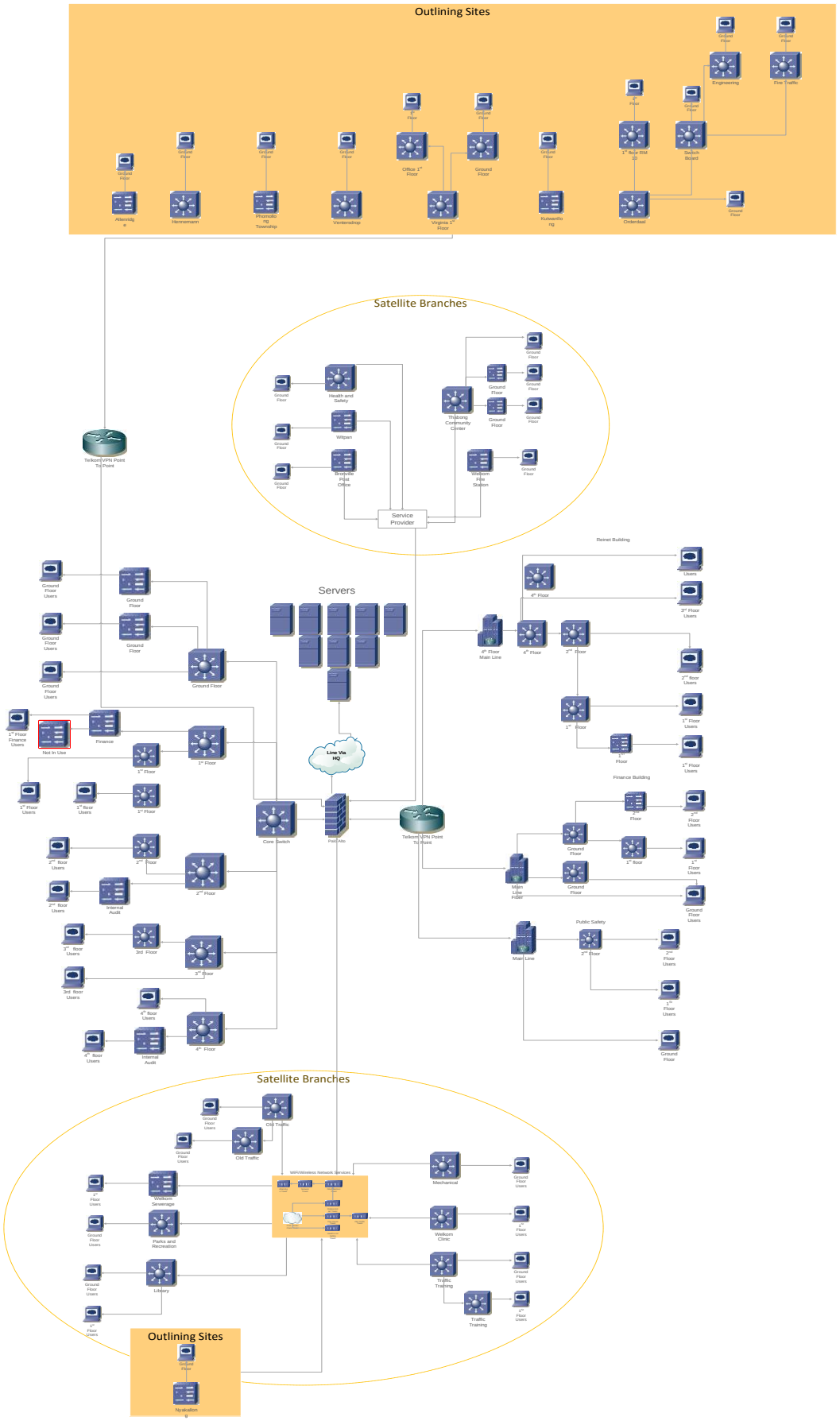

Figure 3: LAN/WAN Network Consolidated

3.6 Summary of Key applications used by the Business Units

MAPPING OF APPLICATIONS vs BUSINESS UNITS	Office of the Municipal Manager	Community Services	Infrastructure Services	LED & Planning	Finance	Corporate Services	Strategic Support Services
Cash Drawer					✓		✓
Syntell			✓		✓		✓
Solar					✓	✓	✓
Telephony	✓	✓	✓	✓	✓	✓	✓
PayDay					✓	✓	✓
Paperless Agenda	✓	✓	✓	✓	✓	✓	✓
Microsoft End User Computing (EUC) and Email Office 365	✓	✓	✓	✓	✓	✓	✓
Critical Network Share Drives	✓	✓	✓	✓	✓	✓	✓

TABLE 4: Key Applications Mapping for Business Units

3.7 ORGANIZATION STRUCTURE

In order to execute the ICT Strategic Plan, the requirement and alignment of the resourcing and challenges for the Matjhabeng ICT Department is a critical success factor. The proposed Organizational Structure

implementation and headcount allocations that is tabled is reflected below:

Figure 4: ICT Organizational Structure

4. STRENGTHS, WEAKNESSES, OPPORTUNITIES AND THREATS (SWOT) ANALYSIS

Strengths, weaknesses, Opportunities and Threats (SWOT) provides a sound introspective mechanism that allows for identification of what the high-level state of the ICT Department is, along with providing a good platform to build a tangible ICT Plan that is executable.

STRENGTHS	**WEAKNESSES**
• Committed and Dedicated ICT Staff • Leadership Commitment to support ICT • Good ability to run operations without defined processes and procedures • Graduate and Learnership development and use for ICT operations	• Not enough staff • Lack of Training and Development of existing staff that causes high reliance on suppliers • Lack of formal processes and procedures which results in limited accountability and measurement of ICT performance • Training lab is inadequate and not fit for purpose • Legacy infrastructure with End of Life (EoL) of technology and limited support and recovery capability
OPPORTUNITIES	**THREATS**
• Evolution of legacy ICT infrastructure and opportunity for the ICT department to gain training to reduce dependence on suppliers and service providers • Executive Management support for ICT modernization • Graduate and Learnership volunteers can development systems to improve ICT service delivery and increased efficiencies	• Temporary Staff poses risks to continued operations and inhibits access to key systems • Permanent Staff are not regularly trained on technology and platforms in use which results in high reliance on Suppliers and risks • Lack of Disaster Recovery Solution will impact the Municipality and revenue collection • Vulnerable systems pose risks to users and municipal data • Administration and User Auditing of key systems not in place which poses fraud risks and no accountability for administrative users • Acting ICT Manager position currently limits authority, direction, planning and uncertainty for the ICT department

TABLE 5: SWOT ANALYSIS

5. GAP ANALYSIS SUMMARY

The GAP analysis is focused on alignment and mapping of the industry best practices relevant to ICT infrastructure, applications and technology currently in place at Matjhabeng. In order to be as precise as possible, attention was placed on application criticality then tiered down towards the underlying infrastructure.

The current gaps are summarized below:

5.1 A number of End of Life (EoL) network devices on the Local Area Network (LAN) and legacy Service and Storage Hardware with no standardization on vendors which has resulted in a multi-vendor environment that poses challenges and risks to operate and support.

5.2 Distances between Patch/Server Rooms and Racks in the Main Campus building Civic Centre is > 100 Meters which will result in degradation and loss of signal on the LAN in some instances this is up to approximately 150 metres.

5.3 Operating systems are outdated including Windows Server 2003, 2008 and 2012R2 which is a high risk for applications that reside on them with no or limited OEM support.

5.4 Limited network utilization visibility and reporting which results in not being able to account for transmission costs, upgrades and forecasting, which also inhibits the ability to guaranty quality of service.

5.5 No Wi-Fi network to reduce reliance on physical LAN cabling infrastructure for Installs, Moves, Additions, Changes and Deletions (IMACD).

5.6 Development of ICT Organizational Structure with additional headcount to ensure efficient and effective execution and support of the ICT Strategic Plan including improvement on day to day support and operations

5.7 Training and development of ICT staff for key systems is not done which has resulted in the ICT Department not being able to do administration on key systems e.g. Firewall, LAN switches.

5.8 Ineffective policies and procedures that are either not developed and/or implemented which results in the lack of accountability due to not having the appropriate controls in place.

5.9 Legacy servers, storage and lack of Disaster Recovery (DR) solution can be detrimental to the Municipality in the event of any disaster and should be prioritized.

5.10 The revitalization of the ICT infrastructure needs to be prioritized and this becomes more crucial to harness ICT to support Local Economic Development (LED), improved access and reliability across the network OS development of additional applications to better support the municipality as a whole.

5.11 Development and execution of Standard Operating Procedures (SOP) to address User Access Control and Audit logging, Change Management, ICT Security, Disaster Recovery and Business Continuity

6. ICT IMPLEMENTATION PLAN

The execution of the ICT Implementation plan has numerous dependencies, however, the guiding principle for this is based on the SHORT-TERM objectives being 1 to 2 years and LONG TERM which is more than 3 years. This then allows for planning and alignment for the 5 year period in a more pragmatic manner along with ensuring a tangible and feasible impact on budgeting and spend forecasting.

6.1 SHORT TERM

6.1.1 Corporate Governance for ICT implementation including Policies, Plans and Procedures.

6.1.2 Applications Service Level Agreement (SLA) alignment to Business expectations and definition of ICT obligations and deliverables.

6.1.3 Operational Level Agreements (OLA) to improve visibility, expectations and delivery to all business units within Matjhabeng Local Municipality.

6.1.4 Definition and application of Key Performance Indicators (KPIs) to have more responsibility and accountability for ICT staff and management along with performance management.

6.1.5 Re-vitalization of legacy and ageing infrastructure including Servers and Storage.

6.1.6 Revamp and readiness of Disaster Recovery Site in Virginia.

6.1.7 Real-time vulnerability assessment solution and evolution of Anti-Virus for EUC and Servers and Operating Systems for threat reduction.

6.1.8 Re-vitalization of LAN switching environment across all sites.

6.1.9 Network Optimization for visibility, control, acceleration of access to key applications and reporting of network level usage.

6.1.10 Wi-Fi deployment for all Matjhabeng Municipal Buildings and offices.

6.1.11 Cloud Readiness and Strategy development focused around Applications and Operating Systems.

6.1.12 ICT Resourcing, training and development.

6.1.13 E-filing of all municipal documents.

6.2 LONG TERM

6.2.1 Expansion of Wi-Fi to Public areas in a phased approach.

6.2.2 Application system upgrades and new features to improve revenue based systems and enhance support based systems

6.2.3 Intra-City broadband planning and implementation.

6.2.4 Harness smart Wi-Fi and broadband for Local Economic Development (LED) and move towards Digital City.

6.2.5 Cloud Implementation Strategy.

6.2.6 Digital Security assessment and implementation.

6.2.7 Online Payment and Virtual Office, to improve access for payments of utility bills etc.

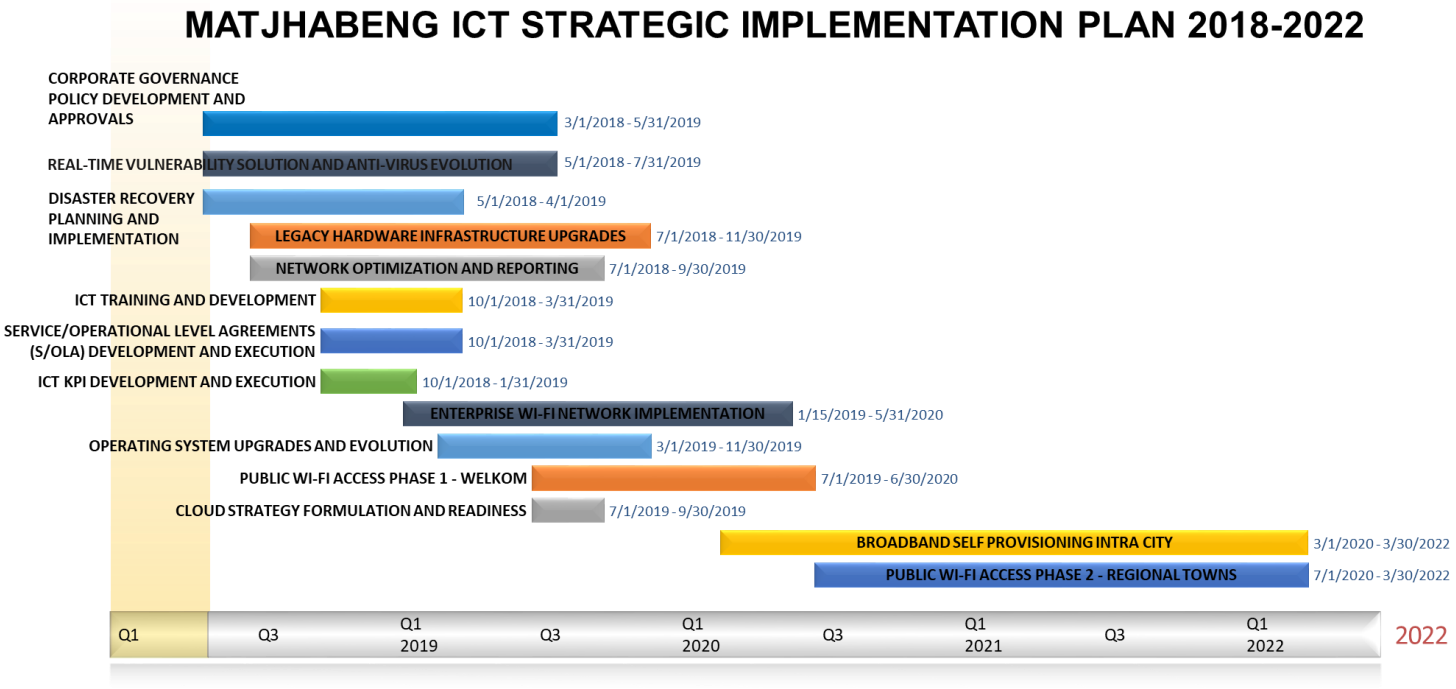

Figure 5: ICT Strategic Plan Implementation 2018-2022

7. APPROVALS