MATJHABENG MUNICIPALITY

ANNEXURES

FOR THE

SECTION 80 POTFOLIO COMMITTEE

FOR

STRATEGIC SUPPORT SERVICES

(IDP)

CONVENED FOR

TUESDAY, 18 SEPTEMBER 2018

AT

10:00

AT

4TH FLOOR ROOM 428, MAIN BUILDING, WELKOM, CIVIC CENT

INDEX

ITEMS FOR DISCUSSION IN THE REVENUE ENHANCEMENT CCOMMITTEE

Purpose: To submit items to REC for consideration

Background

The following items were identified and approved for consideration by the revenue enhancement committee. All these fall within the Strategic Support Services Department and led Mr Makofane until finality or until progress has been achieved. These items are

1. **Fuel**
   The challenge relating to the item was overspending and frustrations to service delivery Departments due to the distance to and from the source. The Municipality has a contract with a service provider for three years but terms and conditions in the contract were not fully implemented. The service provider wanted payment in advance and the Municipality could at all times pay and as a result service delivery failed because trucks could not fill and leave to the field. Hence the source was moved to a willing supplier in Allanridge. The challenge subsequently has been travelling distances from different units in the Municipality.

   Progress

   - The ABSA bank agreed to provide fuel cards for specific vehicles as a temporary solution;
   - The Municipality intends to cancel the contract with the Service provider;
   - An assessment report has been compiled by an independent to resuscitate depots in units as was the case in the past.

2. **Media News**
   The contract has been terminated. The company has resorted to litigating the Municipality regarding the termination.

   Progress
   - We have received papers from the company lawyers and we have briefed our lawyers.

3. **Acquisition of project funds**
   The Municipality has started applying for funds from institutions that provide such funds for projects within municipalities.

   Progress

   - The first application has been made for the neighbourhood Development Project grant via a service provider. There are engagements in terms of progress relating to this fund.

4. Fleet Management

The Municipality has aged fleet and service delivery is hampered. The temporary solution for provision of services was the appointment of private trucks on an as-and-when basis to assist when municipal trucks got damaged. The other recent development was attachment and confiscation of available and working vehicles by office of the sheriff due to outstanding payments the Municipality owed to security companies in our employ. Although payments were made towards the release of the service delivery vehicles, these vehicles were not released and as a result, they still remain with the sheriff.

Progress

- The Municipality has started to litigate against the companies to ensure that they release the vehicles.

5. Monitoring and evaluation (SDBIP)

It is required that each financial year, Municipalities ensure that there are signed SDBIPs that link the use of money for purposes intended and planned. The Municipal SDBIP was signed by the Executive Mayor on the 27th June 2018 for implementation throughout the 2018/2019 financial year. The Department is responsible to monitor project implementation and reporting as per relevant legislation.

Progress

- The Municipal Manager signed his performance agreement with the Executive Mayor before the end of July 2018.
- In the same way as above, each HOD has also signed a performance agreement with the Accounting Officer before the end of July 2018.

6. Risk Management

The Municipality is required to develop a risk management policy, strategy and plan to ensure creation of a risk management and compliance environment. The unit has not yet been established as the last organisational structure did not contain the unit. It is necessary that the Municipality should have a risk register to ensure that challenges of a strategic nature get identified, prioritised and categorised. In the process, we need to have a register that has risks that must be resolved and progress report be provided on a continuous basis.

Progress

The developed risk register is being implemented.

7. Internal Audit

The unit is one of the key and strategic units in the Municipality whose function is to ensure that external audits are done in an improved environment. They are the main players that ensure they provide assurance in terms of performance management and reporting. The Auditor General has never put trust in the internal audit of the Municipality. It is the responsibility of the Municipality to ensure that staff

get capacitated to provide future assurance. One key area was that the Municipality needed to appoint an Audit Committee which was not appointed for 12 months.

Progress

- The Audit Committee was appointed in May 2018

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.

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
Acting ICT Manager: who hereby recommends this ICT Security Policy	Date

Risk Management Implementation Plan

2018/19

Activity	Responsible official or Department	Due date	Outputs / Outcomes
Risk planning			
Detailed risk management implementation plan.	Chief Risk Officer (CRO)	01/07/2018	An approved risk management implementation plan for the financial year 2018/19.
Presentation on Risk Management Awareness, Fraud Risk Awareness to Management.	Chief Risk Officer	30/09/2018	Understanding of Risk Management by Top Management and officials.
Presentation on Risk Management Awareness, Fraud Risk Awareness to operational employees.	Chief Risk Officer	30/09/2018	Understanding of Risk Management operational employees.
Risk orientation (Authorities, structures and responsibilities)			
Appointment of the Chief Risk Officer.	Accounting Officer	01/07/2018	Chief Risk Officer appointed. Formal delegation of risk management responsibilities in writing. Formal delegation of fraud management responsibilities in writing.
Establishment of Risk Management Committee.	Accounting Officer	30/06/2018	Risk Committee Members appointed. Formal delegation of responsibilities to existing committee members via charters.
Orientation of Risk Management Committee.	Accounting Officer	30/07/2018	Completed orientation for all key role players. (Risk Management Committee).
Orientation of Chief Risk Officer.	Accounting Officer	30/07/2018	Completed orientation for all key role players. (CRO)

Activity	Responsible official or Department	Due date	Outputs / Outcomes
Development of Risk management policy, Anti-fraud policy, risk management strategy and fraud prevention strategy.	Chief Risk Officer	01/07/2018	Approved risk management policy, anti-fraud/ prevention policy.
Departmental Risk Profile			
Strategic risk identification, assessment and capturing on Barnowl system and indication of 20 top risk.	Chief Risk Officer	30/09/2018	Approved strategic risk register.
Operational risk identification, assessments and capturing on Barnowl system and indication of 20 top risks.	Chief Risk Officer	30/09/2018	Approved operational risk registers (as per the agreed cycle).
Risk response			
Drafting of action plans for all gaps identified for the top risks, fraud risks.	Risk Owners / CRO	28/12/2018	Action plans implemented per agreed milestone.
Compilation of Risk Assessment Report, Fraud Risk Assessment Report.	Chief Risk Officer	Quarterly	Inform the Accounting Officer about risk assessment of the department, Assisted Internal Audit Planning.
Risk monitoring			
Monitoring effectiveness of mitigation strategies.	Chief Risk Officer	Quarterly	Extent to which mitigating strategies are effective.
Evaluating effectiveness of Risk Management & Fraud Management processes.	Internal / External Audit /	Quarterly	Risk Management & Fraud Management report.

Activity	Responsible official or Department	Due date	Outputs / Outcomes
Accounting Officer's report.	Risk Management Committee Chair	28/02/2019	Report produced as per agreed frequency and content.
Audit committee report.	Risk Management Committee Chair	Quarterly	Report produced as per agreed frequency and content.
Annual report disclosure.	Accounting Officer	15/06/2019	Disclosure in annual report.
Risk management committee report.	Chief Risk Officer	Quarterly	Report produced as per agreed frequency and content.
Monitoring of the RMIP of Municipality.	Chief Risk Officer	Quarterly	

PREPARED BY:	**REVISED BY:**	**ACCEPTED BY:**
ACTING SENIOR ACCOUNTANT	DIRECTOR:	
RISK MANAGEMENT	STRATEGIC SUPPORT SERVICES	MUNICIPAL MANAGER
Name **Puleng Sefuthi**	**T. B. Makofane**	**Mr E. T. Tsoaeli**
Signature ……..	----------	…….
DATE ……...	----------	

MATJHABENG LOCAL MUNICIPALITY

OFFICE OF THE MUNICIPALITY MANAGER

SUB-DIVISION: INTERNAL AUDIT

THREE YEAR ROLLING PLAN

2018-2021

INTERNAL AUDIT PLAN

Table of Contents **Page**

MATJHABENG LOCAL MUNICIPALITY
INTERNAL AUDIT PLAN: 2018/19 – 2020/21

9. 1. INTRODUCTION

9.1 1.1 Terms of Reference

Paragraph 3.2.7 of the Treasury Regulations, requires Internal Audit to prepare in consultation with and for approval by the Audit Committee:

a) A rolling three-year strategic internal audit plan based on its assessment of key areas of risk for the Municipality, having regard to its current operations, those proposed in its strategic plan and its risk management strategy; and

b) An annual internal audit plan for the first year of the rolling three-year strategic internal audit plan.

Standard 2010 of International Standards for Professional Practice of Internal Auditing requires the Chief Audit Executive to establish risk-based plans to determine the priorities of the Internal Audit Activity which are consistent with the municipality objectives and goals.

9.2 1.2 Internal Audit Mandate

Section 165 (2) of the Municipal Finance Management Act, stipulates the following: The internal audit unit of a municipality must.

- The aim is to incorporate all key risk areas into the strategic internal audit plan to ensure that all high risk areas are covered over a three year period 2018 – 2021.
- The objective of this process is to prepare an Internal Audit plan, in consultation with the audit committee.
- Provide guidelines on the activities of Internal Audit Municipality
- Prepare a risk based audit plan and an internal audit program for each financial year.
- A rolling three year strategic internal audit plan based on an risk assessment considering its current operations
- An annual internal audit plan for the first year of the rolling plan.
- Advise the accounting officer and report to the audit committee on the implementation of the internal audit plan etc.

9.3 1.3 Purpose of this Document

This document sets out the Internal Audit Plan for the period 2018/19 to 2020/21 for consideration and approval by the Audit Committee. The plan incorporates the:

- Three-year rolling Strategic Plan the period 2018/19 to 2020/21 ; and
- Annual Internal Audit Plan for the financial year ending 30 June 2019.

The Internal Audit Plan is designed to provide the scope of Internal Audit Activities for the three year period.

It should be noted that the plan is intended to be a life document, thus changes in circumstances may warrant changes to the plan. All such changes to the plan will be communicated to Management for noting and Audit Committee for consideration and approval. Furthermore The Internal Audit Plan for the Matjhabeng local municipality was designed to provide an independent, objective assurance and advisory service, in an efficient and effective manner, to the following key stakeholders:

- the municipality's Council through the Audit Committee of the municipality
- Municipal Manager; Local line management;
- Audit Committee.

The overall approach was to formulate a risk-based Annual Internal Audit Plan to align the priorities of the Internal Audit function with the strategic objectives and goals of the Matjhabeng Local municipality and the related strategic and major business risks as identified by management and the Auditor General

10. 2. INTERNAL AUDIT – ROLES AND RESPONSIBILITIES

The institution of Internal Auditors defines internal audit as follows:

10.1 "… An independent objective assurance and consulting activity designed to add value and promote organization's operations. It helps an organization to accomplish its objectives by bringing as systematic, discipline approach to evaluate and improve the effectiveness of risk management, control and governance processes."

The Internal Audit Activity evaluates and contributes to the improvement of risk management, control and governance systems. Internal Audit Activity adopted a risk-based audit approach and it subscribes to the Code of Ethics of the Institute of Internal Audit and it strives to conduct the reviews according to the International Standards for the Professional Practice of Internal Auditing as well as relevant Government Legislative Framework

10.1.1 2.1 Scope of Internal Audit Activity

The scope of this planning process is to ensure that the regulatory audit plan is implemented

- Three year strategic internal audit plan; and
- One year regulatory internal audit plan.

The following steps will be taken to ensure the effective implementation of the internal audit plan:-

- The results of the risk assessment will be used as a basis for drafting the regulatory audit plan;
- Identify and assess risk at the beginning of each internal audit assignment, and design control testing procedures accordingly;
- Update and maintain the database of risks for the purpose of internal audit coverage through the following:
  - The performance of assurance reviews;
  - Information provided by management; and
  - Information obtained from external audit reports and management reports.

The implementation and execution of the strategic rolling internal audit plan and the annual internal audit plan will be done within the framework of the municipality's Internal Audit charter and as per professional practice of internal auditing. The scope of the execution of the annual internal audit plan will be influenced by the availability of resources in the internal audit section.

2.2 Annual Budget:

The annual budget allocations for Internal Audit Budget for 2018/19 period are shown in the table below:

a. Annual Budget

The three- year budget of the Internal Audit Unit is as follows:

BUDGET	Budget 2016/17	Budget 2017/18	Budget 2018/19
	R	R	R
Total Expenditure	3 718 015,00	3 926 223,00	3 936 064,00

11. 3. STRATEGIC OVERVIEW OF THE MUNICIPALITY

11.1 3.1 Vision and Mission

The vision of the Municipality is "To provide through good governance an effective and efficient people-centered administration that will facilitate the developmental role of local government, taking into account our cultural diversity and improvement of service delivery to our rural and urban communities.

The mission to reach this vision will include

- Maximize efficient and effective utilization of resources to achieve a viable and developmental local government.
- Improve the quality of life of residents and customers by providing quality, accessible and affordable services.
- Deliver sustainable services.
- Improve Community – Council relationships through frequent interaction.
- Provision of capacity to local communities.
- Promotion of social and economic development.
- Creation of a safe and healthy environment.
- Encouragement of communication and participation.
- Implementation of the IDP.
- Adequate training and development of staff and political office bearers.
- Promoting the culture of unity and diversity.
- The promotion of tourism, our natural and historical heritage.

11.2 3.2 Management Responsibilities

Management is responsible for the establishment and maintenance of an effective system of governance, risk management and internal controls. The objectives of the system of internal controls are, *inter alia*, to provide management with reasonable, but not absolute assurance that:

- Risks are properly managed;
- Assets are safeguarded;
- Financial and operational information are reliable;
- Operations are effective and efficient; and
- Laws, regulations and contracts are complied with.

The principal safeguard against fraud, misstatement and irregularities is an effective system of internal controls. It must, however, be rec0ty.ognised that there are inherent limitations in any

system of internal controls, including human errors and circumventions through collusions. The prevention and detection of fraud therefore, remains management's responsibility.

11.3 3.3 Legislative Mandate

The following is some of the national laws and regulations that govern the Municipality:

11.3.1 3.3.1 Core- Business related legislation

- Constitution of the republic of South Africa, 1996
- Local Government Municipal Demarcation Act, No.27 of 1998
- Local Government Municipal Structures Act, No.117 of 1998
- Local Government Municipal Systems Act, No.32 of 2000
- Local Government Municipal Financial Management Act, No 56 of 2003
- Local Government Municipal Property Rates Act, No. 6 of 2004

11.3.2 3.3.2 Administrative Legislation

The Municipalities' administrative functions are regulated by a number of the following national transversal laws and regulations:

Employment Equity Act, 1998 (Act No. 55 of 1998)

Preferential Procurement Policy Framework Act, 2000 (Act No. 5 of 2000)

Labour Relations Act, 1995 (Act No. 66 of 1995)

Basic Conditions of Employment Act, 1997 (Act No. 75 of 1997)

Skills Development Act, 1998 (Act No. 97 of 1998)

Municipal Financial Management Act, No 56 of 2003

Division of Revenue Act (Annually)

National Archives Act (Act No. 43 of 1996)

Occupational Health and Safety Act (Act No. 85 of 1993)

Collective Agreements

Treasury Regulations

11.4 4 Basis for the Plan

The plan was prepared based on:

- Auditor-General Management letter.
- The plan does takes into account any additional management requests that may be received during the year by making hours available for any special/ad hoc requests to be received.

TABLE A

12. THREE-YEAR ROLLING INTERNAL AUDIT PLAN

No.	*Programme/Subprogramme*	*Business Process*	*Inherent Risks*	*2018/19 Year*	*2019/20 Year*	*2020/21 Year*
1.	Financial Accounting/Reporting	Financial Statements Review	□ Compulsory/ Mandatory	√	√	√
2.	Revenue	Revenue	• Follow up on prior year: Revenue: Service Charges • Revenue: Property rates: Properties not being billed for property rates • Revenue: Property rates: Tariff codes used differ from usage codes • Revenue (Service Charge): Meter reading • Revenue (Service Charge): Sewerage and Refuse charges • Revenue (Other income):Fresh Produce • Revenue (Other income) Rental income • Revenue (Other Income): Rental of facilities Revenue (Service Charge):	√	√	√

No.	Programme/Subprogramme	Business Process	Inherent Risks	2018/19 Year	2019/20 Year	2020/21 Year
3.	Supply Chain Management and Budget and Expenditure	Supply Chain Management and Budget and Expenditure	• Awards were made to providers who are in the service of other state institutions or whose directors or principal shareholders are in the service of other state institutions, in contravention of MFMA 112(j) and SCM regulations • Deviations from Procurement policy as a result of e.g. emergency, sole provider of services • Bidding Process • Composition of Bid Committees	√	√	√

No.	Programme/Subprogramme	Business Process	Inherent Risks	2018/19 Year	2019/20 Year	2020/21 Year

4.	Assets Management	Assets Management	• Immovable assets: Physical verification. • Movable Assets - Disposals • Movable Assets - Physical Verification • Movable assets: Additions Movable assets:	√	√	√

No.	Programme/Subprogramme	Business Process	Inherent Risks	2018/19 Year	2019/20 Year	2020/21 Year
5	Performance	Performance Information	• POEs: Completeness • Pre-Determined Objectives- Key performance indicators and targets were not set for all priorities/objectives in the IDP. • Pre-Determined Objectives: Difference between reported and audited performance achievement • Pre-determined Objectives: No consistency between planned and reported priorities/objectives • Pre-Determined Objectives: Performance indicators/measurement not well-defined	√	√	√
6.	Information Technology	Information Technology Services	• General IT controls: Information technology governance • General IT controls: Information technology service continuity • General IT controls: Security management • General IT controls: User access management	√	√	√
7.	Risk Management	Risk Management	• Risk Management process • Risk Management policy • Risk Management Strategy	√	√	

13. 5. AUDIT STAFF

The approved Organizational Structure of the Internal Audit Units comprises of the following positions:

Position	Status	**Academic Qualification**
1. Manager	Filled	B.Com, Forensic and Investigative Audit; Municipal Finance Management Programme
2. Senior Internal Auditor : Performance	Filled	B.Com, CPMD Programme in forensic and investigative auditing Programme in Risk management
3. Senior Internal Auditor: Operational	Vacant	-
4. Internal Auditor	Filled	B.Com, Certf in Computer Auditing, Programme in forensic and investigative auditing

5. Internal Auditor	Filled	B.Tech, Municipal Finance Management Programme Programme in forensic and investigative auditing Programme in Risk management
6. Internal Auditor	Filled	B.Tech (internal audit), Btech (project Management)
7. Internal Auditor	Vacant	-
8. Internal Auditor	Vacant	-
9. Internal Auditor	Vacant	-
10.Internal Auditor	Vacant	-
11.Internal Auditor	Vacant	-
12.Internal Audit clerk	Vacant	-

14. 6. AUDIT HOURS AVAILABLE

	Projected Hours
Manager	**782,00**
Senior Internal Auditor	**1912,00**
Internal Auditor	**1912,00**
Internal Auditor	**1912,00**
Internal Auditor	**1912,00**
Total Hours for the year	**8430,00**
Less Holidays	**590,00**
Less Leave Days	**843,00**
Actual Audit Hours available	**8177,00**

15. 7. AUDIT UNIVERSE – 2018/19

An audit universe represents the potential range of all audit activities and is comprised of a number of auditable entities. These entities generally include a range of programs, activities, functions, structures and initiatives which collectively contribute to the achievement of the municipal strategic objectives.

Components of the Audit Universe are identified as functions of the Municipality. This has been selected in order to ensure the alignment of the internal audit activities with the objectives of the Municipality. Over and above the functional areas identified as elements of the audit universe, there are mandatory audits that must be performed as required by legislation or resolutions of council. The Table below depicts different basis for identification of mandatory elements of the audit universe:

No	Auditable Area	Basis for Identification
1.	Risk Management	Municipal Finance Management Act requires that Internal Audit must advise the accounting officer and report to the Audit committee on matters relating to risk and risk management.
2	Governance	IIA standards definition of the Nature of Work of the Internal Audit.
3.	Performance Information	Section 165 of Municipal Finance Management Act requires that Internal Audit must advise the accounting officer and report to the audit committee on matters relating to performance.
4.	Compliance with Acts, policies and Legislation	Section 165 of Municipal Finance Management Act requires that Internal Audit must advise the accounting officer and report to the audit committee on matters relating to compliance with acts, legislations and policies.

8. ANNUAL INTERNAL AUDIT PLAN 2018/19

16. APPROACH

All risks rated high were selected and included for audit in the Internal Audit Plan for 2018/19. Those are the risks that are likely to happen or likely to occur more than once, and will have critical and negative outcomes to the achievement of the objectives.

The prioritisation was also made based on the capacity/human resources within the Internal Audit unit. The audit hours were therefore allocated in terms of available personnel in the audit unit.

17. TABLE B ANNUAL INTERNAL AUDIT PLAN 2018/19

Project	Auditable Process	Auditable Process	Audit Objective	COMPLIANCE	FINANCIAL	OPERATIONAL	PERFORMANCE	FORENSIC	TOTAL HRS
1.	Risk Management Audit.	• Identification of Risks: Strategic, Operational & Compliance. • Assessing the risks: Strategic, Operational & Compliance. • Preparation of risk register	To review and evaluate the effectiveness and efficiency of Risk management processes and operations; as designed and implemented by Management; as well as its compliance to applicable Acts and Regulations.	X		X			344

Project	Auditable Process	Auditable Process	Audit Objective	COMPLIANCE	FINANCIAL	OPERATIONAL	PERFORMANCE	FORENSIC	TOTAL HRS
2.	Compliance and Governance Review	Ensure compliance to all applicable legislation, Acts and policies	Review financial and operation processes to verify compliance to applicable Acts, Policies and Legislations.	X	X	X			1496
3	Monitoring of Audit action Plan	Ensure that all the issues that have been raised by Auditor General are addressed	To review the adequacy and effectiveness of controls aimed at compliance with relevant financial and Operational laws, Acts and regulations	X	X	X	X		

Project	Auditable Process	Auditable Process	Audit Objective	COMPLIANCE	FINANCIAL	OPERATIONAL	PERFORMANCE	FORENSIC	TOTAL HRS
4.	Performance Audit Q1-Q4	• Audit of performance information. • basic service delivery • KPA2:municipal transformation and organizational development • KPA 4: good governance and public participation • kpa3:municipal financial viability and management • KPA 5: local economic development	To rev the adeq and effectiver of operati systems desig to ach ieve Municipal objectives and applicable compliance with laws and regulations.	X	X	X	X		888

5.	Supply Chain Management	• SCM Policy • Supplier Data Base • Bid Committees • Bid Tendering Process • Declaration of Interest	To review the operational adequacy; efficiency and effectiveness of controls meant to ensure compliance with laws and regulations	X	X	X			800

Project	Auditable Process	Auditable Process	Audit Objective	COMPLIANCE	FINANCIAL	OPERATIONAL	PERFORMANCE	FORENSIC	TOTAL HRS

6.	Expenditure	• Payment Period • Creditors Reconciliation • Payment Authorization • Funds Verification against budget	To review and evaluate the operational adequacy; efficiency and effectiveness of controls meant to ensure compliance with laws and regulations in Expenditure	X	X	X			824
7.	Revenue	• Connections. • Billing & Invoicing. • Other Income. • Reconnections. • Disconnections. • Tariffs.	To review and evaluate the operational adequacy; efficiency and effectiveness of controls meant to ensure compliance with applicable laws and regulations. in Revenue section.	X	X	X			512
9	Contract Management/ Legal	□ Contract Management Register Completeness.	To review the adequacy and effectiveness of controls and	X	X	X			344

Project	Auditable Process	Auditable Process	Audit Objective	COMPLIANCE	FINANCIAL	OPERATIONAL	PERFORMANCE	FORENSIC	TOTAL HRS
			evaluate compliance with applicable laws and regulations.						
10	Information Technology	• Security Management • Information technology governance • User access management • Information technology disaster management plan	To review and evaluate the operational adequacy; efficiency and effectiveness of controls meant to ensure compliance with applicable laws and regulations.	X		X			528
11	Asset Management	• Fixed Asset Register • Asset Register GRAP Compliance • Additions • Disposals • Recording and movement of inventory	To review the adequacy and effectiveness of controls and determine compliance with policies and regulations	x	x	x			840

		• Safe keeping of inventory							

18. 9. REPORTING

Communication, particularly through reports, is an essential element of the internal audit process. Reports will clearly demonstrate the control and operating concerns identified from the audit, the cause and potential impact thereof, reasoned recommendations for change and agreed programme of action.

The Internal Audit Function will report quarterly to the Audit Committee and regularly to the Accounting Officer on the achievement of the plan based on the available resources.

19. 10. RESTRICTION ON DISTRIBUTION OF THIS PLAN

This plan has been prepared for the sole and exclusive use of the Municipality and may not be made available to anyone other than authorized persons within the Municipality, nor relied upon by any third party without the prior written consent of the Audit Committee.

20. 11. APPROVAL OF THE PLAN

This plan is prepared by the Manager: Internal Audit and respectively discussed and agreed with the Executive Management and presented to the Audit Committee for approval.

Information Communication and Technology (ICT) Strategic Plan

Matjhabeng Local Municipality

Document Version: 0.5 (Draft)

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

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.

21. 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

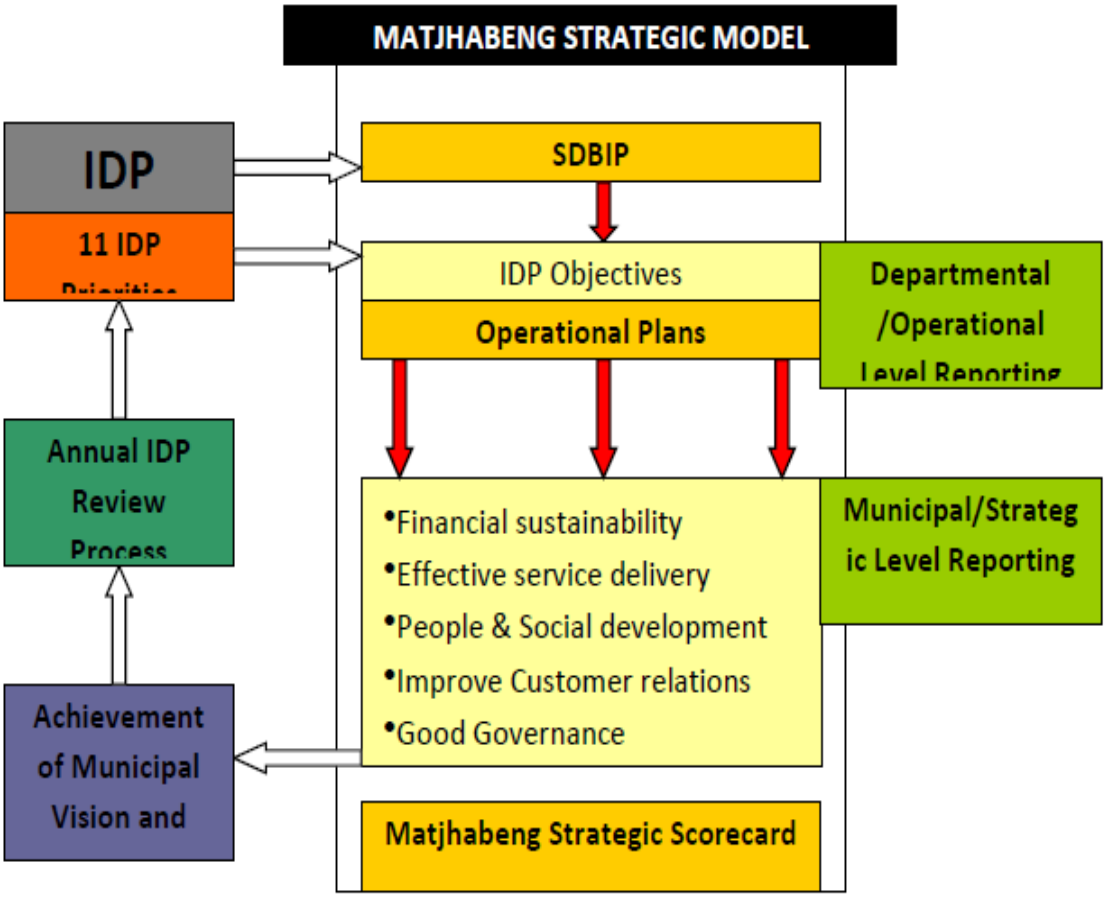

Figure 1: Matjhabeng strategic model from IDP

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:

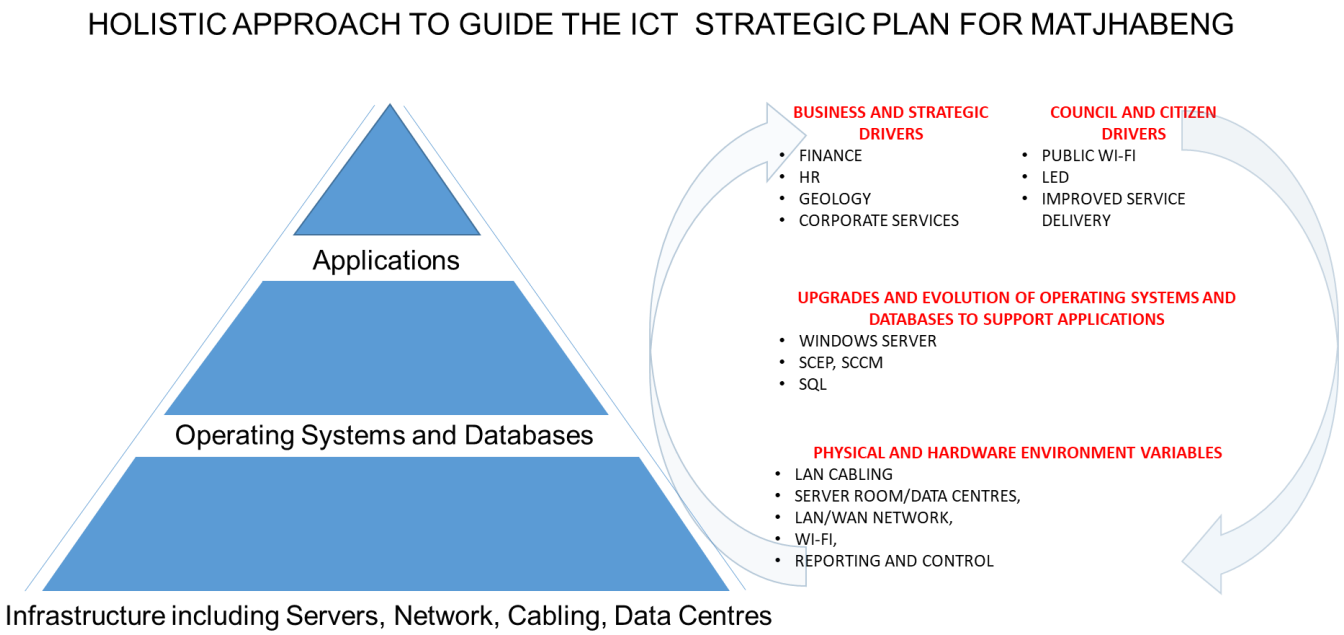

Figure 2: Strategic plan drivers

22. 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:

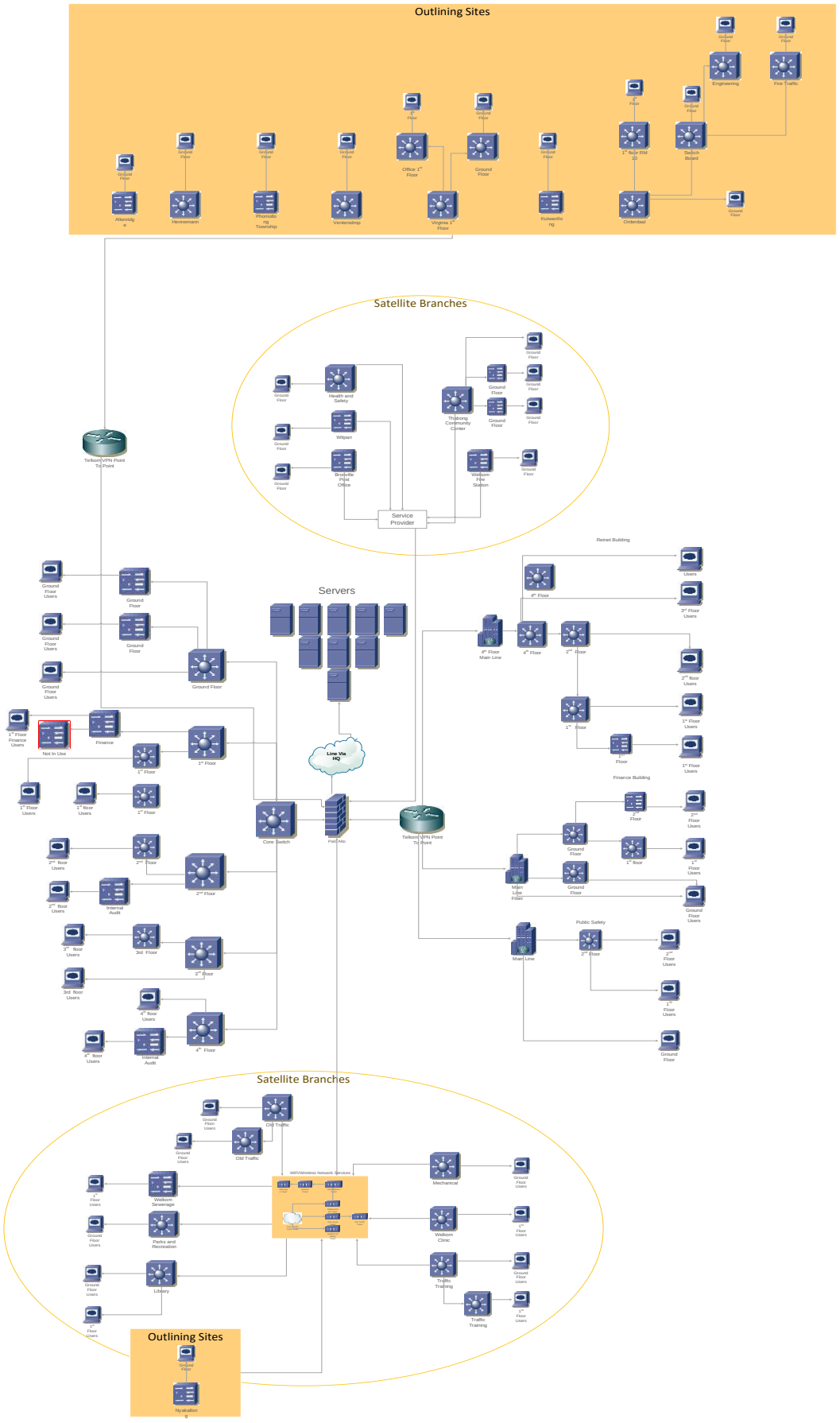
Outlining Sites
Satellite Branches
Service Provider
Servers
Line Via HQ
Core Switch
Satellite Branches
Outlining Sites

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:

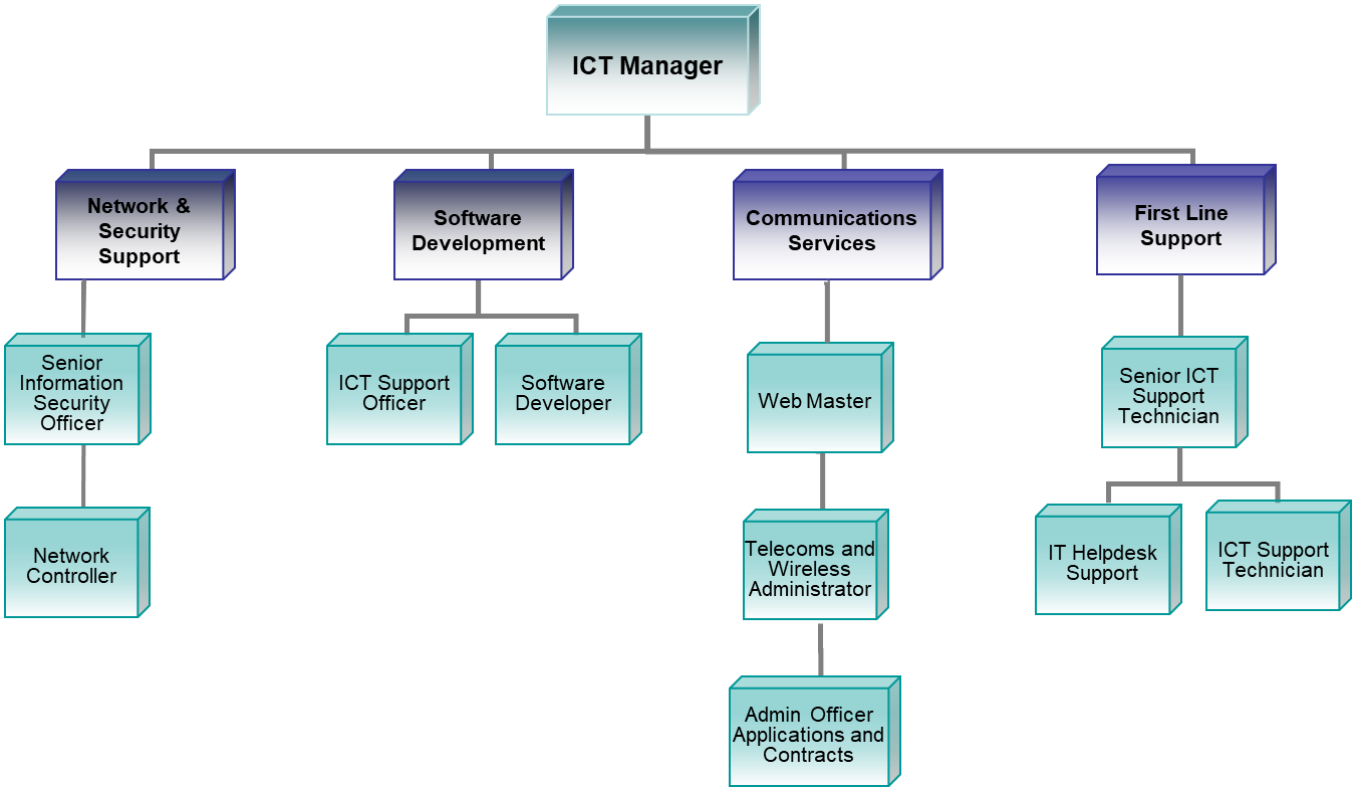

Figure 4: ICT Organizational Structure

23. 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

24. 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

25. 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.

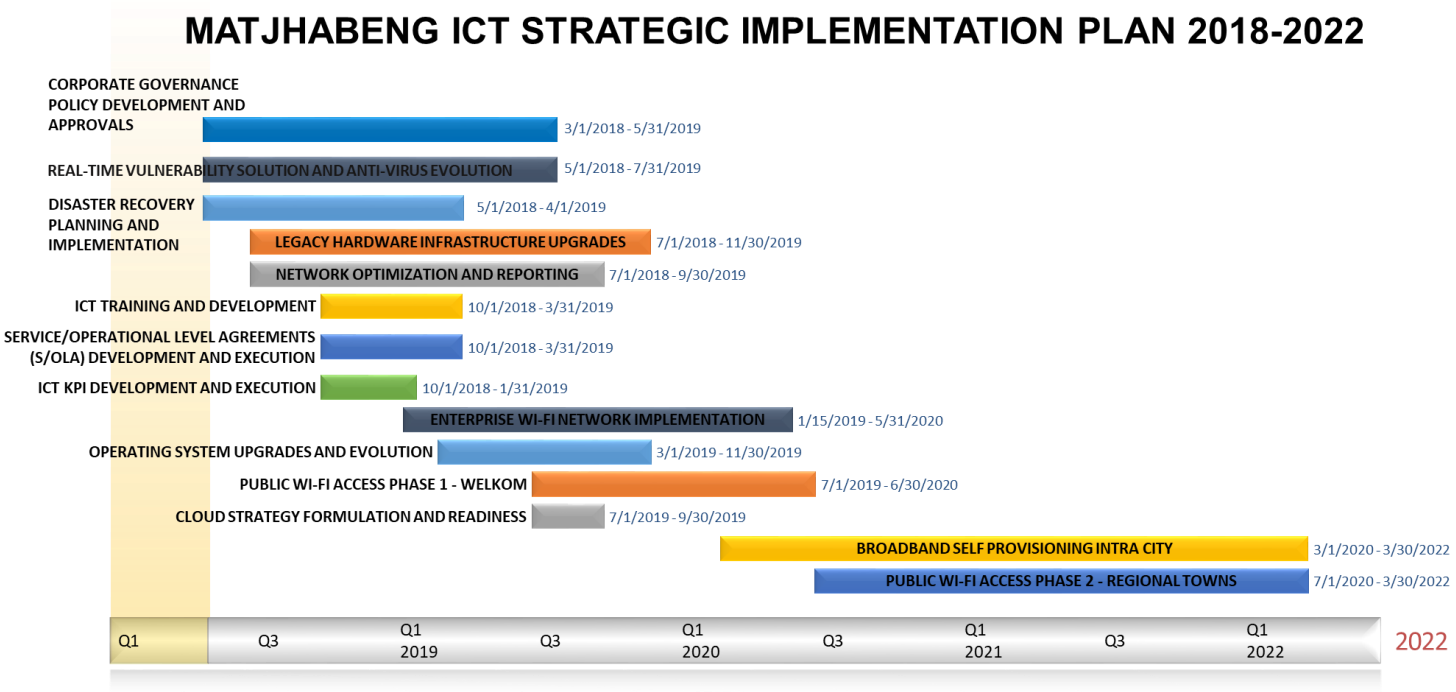

Figure 5: ICT Strategic Plan Implementation 2018-2022

26. APPROVALS

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 IT Strategic Plan	Date
Executive Director: SSS, who hereby recommends and approves this IT StrategicPlan	Date
Acting ICT Manager: who hereby recommends this IT Strategic Plan	Date