Information Communication and Technology (ICT)

CHANGE MANAGEMENT POLICY

Matjhabeng Local Municipality

(MLM)

Contents

1. INTRODUCTION

Matjhabeng Local Municipality (MLM) is reliant on Information, Communications and Technology (ICT) to ensure service delivery requirements to the communities are met, specifically for key systems like Solar, PayDay, Syntell, Cashdrawer, Email and Inter/Intranet.

The purpose of this document is to ensure that MLM manages change in a clear and concise manner whilst ensuring that business impact and downtime is accounted for and managed in a hierarchical way. Changes on key ICT systems that are as a result of failures, upgrades, enhancements can potentially lead to disasters if not managed effectively hence the overarching purpose of this document to provide the directive and rules around how change is managed within MLM.

The importance of change management and controls to mitigate downtime has become increasingly important and is underlined by the following:

- Failure in Business systems that rely on ICT to collect rates, taxes and utility-based services has a direct impact to finances of the municipality.
- The inability to recover from failures, changes or incidents due to unplanned changes.

2. OBJECTIVE AND PURPOSE OF THE POLICY

The objective of this policy is to define change management and controls for the MLM ICT Information Systems, Infrastructure, Users and Service Providers. This policy seeks to ensure that compliance to change management based on guidelines and best practices is achieved effectively.

3. SCOPE

The ICT Change Management is applicable to all users in the MLM, including its service providers and/or vendors. This policy is regarded as being crucial to the changes and incidents in MLM that affect ICT systems. The policy covers the following domains:

- Planned changes.
- Unplanned changes (Emergencies).
- Upgrades or enhancements to existing ICT systems (Major Changes).
- Incidents due to disasters, outages or other events.

4. TERMS AND ABBREVIATIONS

MLM	- Matjhabeng Local Municipality
ICT	- Information, Communications and Technology
CCAF	- Change Control Application Form
CCF	- Change Control Forum

5. CHANGE MANAGEMENT POLICY

All changes must be completed using the CCAF in Annexure 1 and the CCF is responsible for oversight, implementation and monitoring of ICT changes. The change management scenarios are classified based on the following definitions that must be adhered to:

5.1 PLANNED CHANGES

This includes installations, moves, additions, upgrades/downgrades and decommission of all hardware, software and physical ICT infrastructure equipment and should include the following items:

- Detailed description of the change completed in the Change Control Application Form (CCAF)
- The impact to business critical or non-business critical systems.
- The configuration that will be done e.g. command line changes, software changes etc.
- Test plan if applicable and possible.
- Information of the change should be reported as an item to the Change Control Forum (CCF).
- Roll back plan.
- Implementation outcomes are recorded and part of item for the CCF.

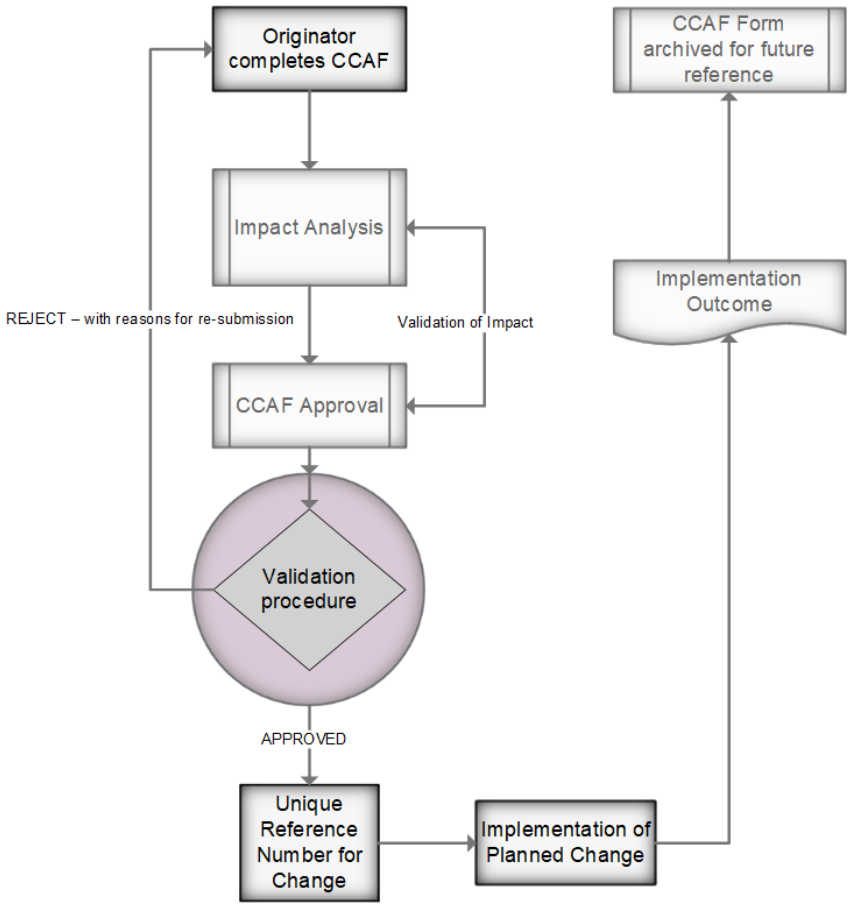


DIAGRAM 1 – PLANNED CHANGES WORKFLOW

5.2 EMERGENCY CHANGES

This includes service affecting changes that need to be implemented with priority due to severity and impact of ICT systems affected and should include the following items:

- Reason for emergency.
- Detailed description of the change.
- CCF Approval.
- The impact analysis on the business-critical system affected.
- The configuration that will be done e.g. command line changes, software changes etc.
- Test plan including procedure for validating that system functionality is working as expected including end user testing.
- Roll back plan (if possible).
- Escalation and Executive management approvals.
- Implementation outcome and reporting to the CCF.

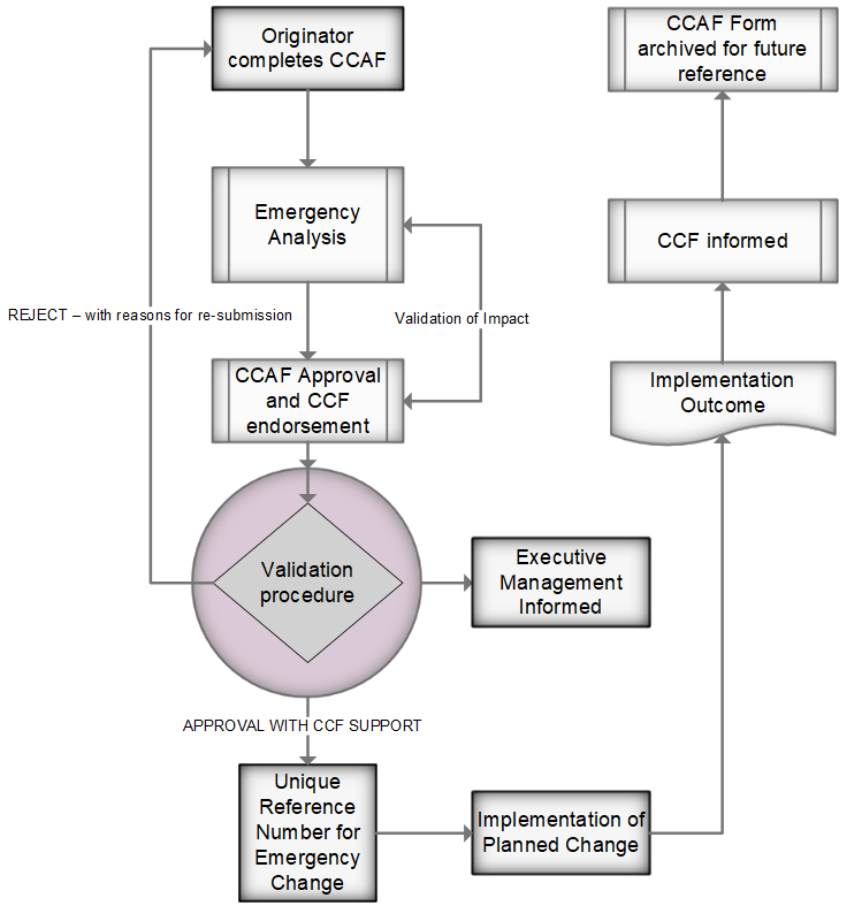


DIAGRAM 2 – EMERGENCY CHANGES WORKFLOW

5.3 INCIDENT MANAGEMENT

In the event of major outages due to incidents within the MLM ICT environment there may be a need to have clear change management procedures to mitigate the disruption to MLM business processes, the procedure to manage such incidents should include the following:

- Incident detection and recording.
- Incident reporting and communication.
- Classification of Priority based on service impact.

- Investigation and analysis.
- Resolution and record keeping.
- Incident closure and reporting.
- Incident ownership, monitoring, tracking and communication.
- Mitigation plans and reporting to the CCF.

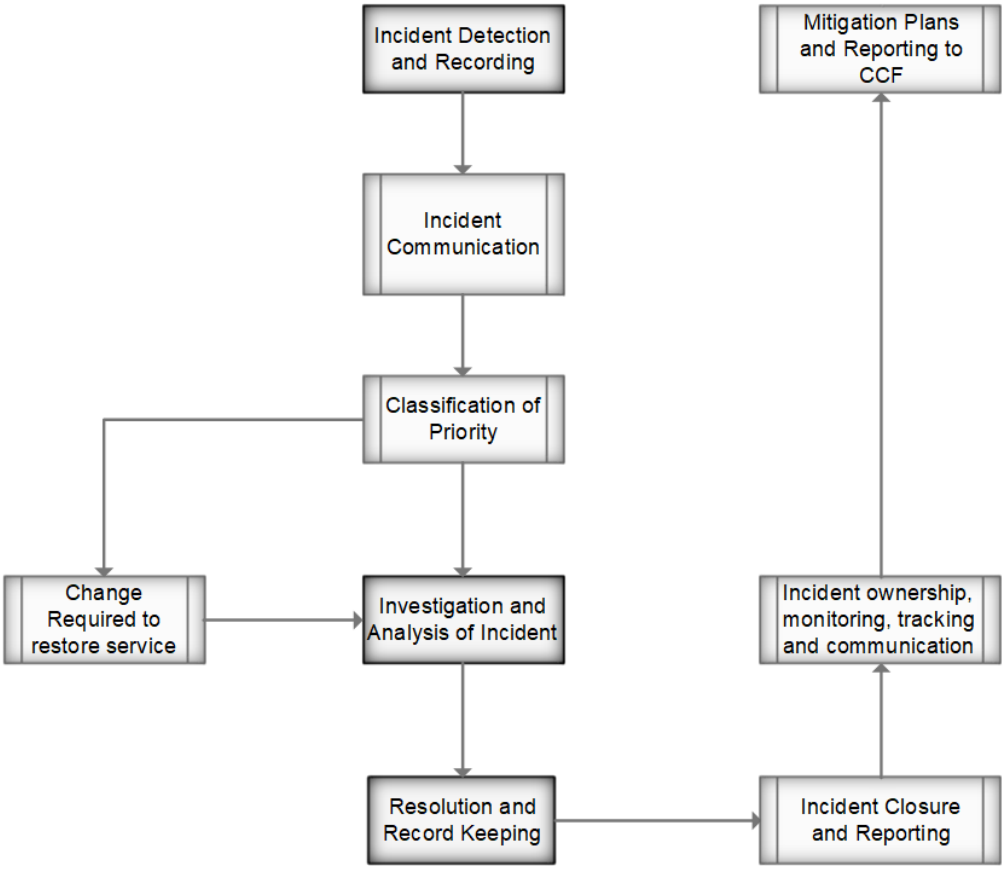


DIAGRAM 3 – INCIDENT MANAGEMENT WORKFLOW

5.4 MAJOR CHANGES (SOFTWARE RELEASES AND/OR HARDWARE)

A Major Change may be classified as a situation which can result in loss of a key application that the municipality requires with the added impact of requiring changes including but not limited to software/hardware upgrades or application based changes in order to restore service back to normal operations.

Major Changes should include the following items:

- The originator completes the detailed description of the change in the CCAF.
- Reason for the Major Change.

- The impact analysis on the business-critical system affected.
- Approval from the CCF.
- The configuration that will be done e.g. command line changes, software changes etc.
- Test plan including procedure for validating that system functionality is working as expected including end user testing.
- Roll back plan.
- Implementation outcome and reporting to the CCF.

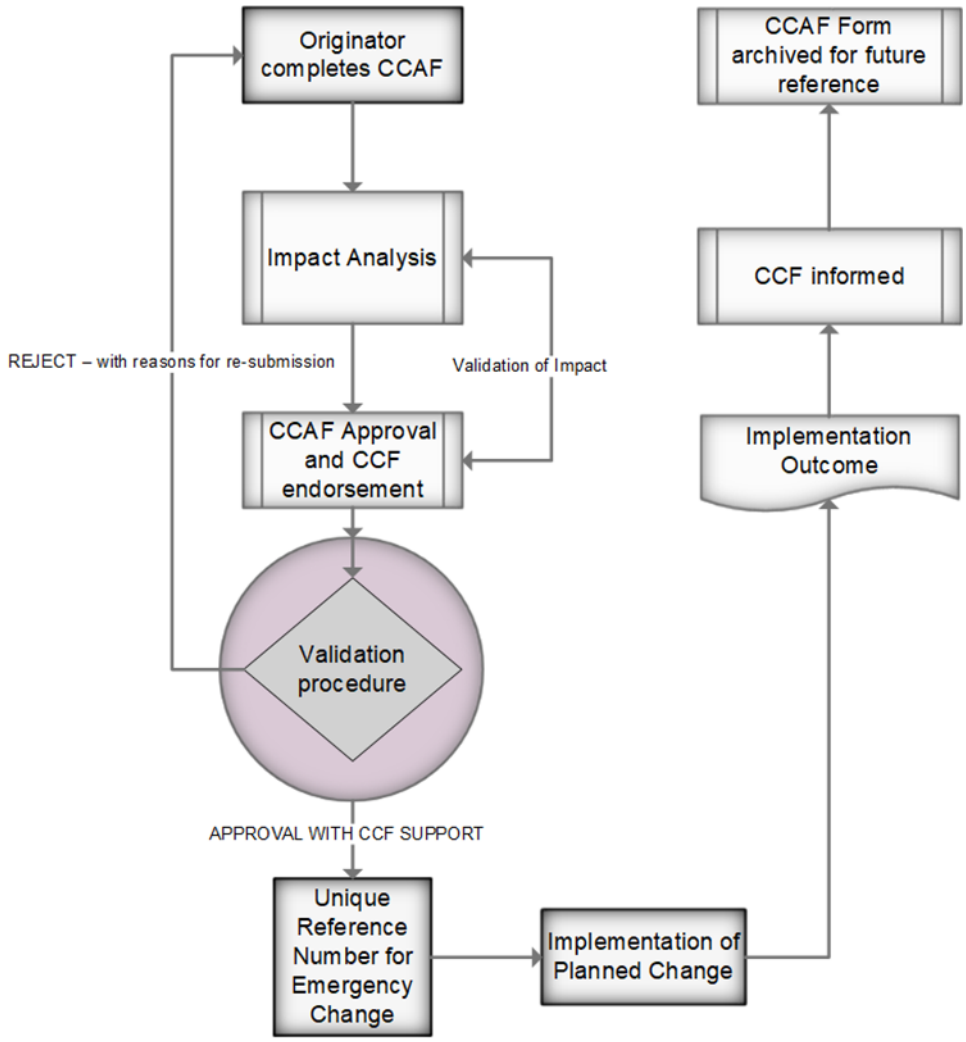


DIAGRAM 4 – MAJOR CHANGES WORKFLOW

6. CHANGE CONTROL FORUM (CCF)

The Change Control Forum will oversee the change control policy, processes and monitoring. The CCF will review and when necessary approve changes that are Major or Emergencies. The purpose of the CCF is to ensure that change management procedures and processes are adhered to in order to ensure sound governance practices for Change Management.

6.1 CCF COMMITTEE MEMBERS

The CCF shall have the following members:

- ICT Manager (Chair Person);
- Risk and Audit representative;
- Network Administrator;
- Systems Administrator;
- Security Administrator;

For the purpose of completeness and visibility the CCF may change the members and include Executive management for inputs and approvals for emergency and major changes.

7. LEGAL FRAMEWORK

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

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

- Constitution of the Republic of South Africa Act, Act No. 108 of 1996;
- Copyright Act, Act No. 98 of 1978;
- Electronic Communications and Transactions Act, Act No. 25 of 2002;
- Minimum Information Security Standards, as approved by Cabinet in 1996;
- Municipal Finance Management Act, Act No. 56 of 2003;
- Municipal Structures Act, Act No. 117 of 1998;
- Municipal Systems Act, Act No. 32, of 2000;
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996;

- Promotion of Access to Information Act, Act No. 2 of 2000;
- Protection of Personal Information Act, Act No. 4 of 2013;
- Regulation of Interception of Communications Act, Act No. 70 of 2002; and
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005.

8. APPLICABILITY AND ADHERENCE

This Policy is applicable to all employees of MLM along with Service Providers and Sub-contractors that are responsible for ICT systems inclusive of hardware and software within the MLM ICT environment. Failure to comply with the provisions as set out above or any amendment thereto, shall be subjected to appropriate disciplinary action.

Change Control Application Form (CCAF)
Matjhabeng Local Municipality ICT Department

Reference No.	

Applicants Information

Department/Service Provider		
Address	Street Number	
	Street Name	
	City/Town	
	P.O. Box	
	Suburb	
	City/Town	
	Postal Code	
Contact Details	Contact Person	
	Contact No.	
	Alternative Tel. No.	
	Email Address	
	Facsimile No.	

Configuration Change Request Detail

Description of Request			
Impact of Request			
Environment Affected			
Dependencies Impacted			
Date Change Required		Time Change Required	

ICT Authorization / CCF

Requested By		Date Requested	
Approved By		Date Approved	

Technician/Administrator/Supplier Resource

Responsible Engineer						
Potential Risks						
Authorisation	Authorised (Y/N)	By		Not Authorised (Y/N)	By	
		Date			Date	

Escalation

ICT Manager	Date		Time	
Executive: SSS	Date		Time	
Municipal Manager(MM)	Date		Time	

Roll-back Plan (where applicable)

Audit Trail

Before Image	Date		Time	
After Image	Date		Time	

Information Communication and Technology (ICT)

Matjhabeng Local Municipality

(MLM)

IT Disaster Recovery (DR) Strategy

Table of Contents

Document Information

Project Name:	ICT DR and BCP Matjhabeng		
Prepared By:	Matjhabeng ICT	**Document Version No:**	0.5
Title:	DR and BCP for Matjhabeng ICT	**Document Version Date:**	01/08/2018
Reviewed By:		**Review Date:**	

Distribution List

Name	Date	Phone/Fax/Email

Document Version History

Version Number	Version Date	Revised By	Description	Filename
0.1	11/04/2018	Matjhabeng ICT	Document creation	DR and BCP for Matjhabeng
0.2	27/04/2018	Matjhabeng ICT		
0.3	12/05/2018	Matjhabeng ICT		
0.4	07/06/2018	Matjhabeng ICT		
0.5	01/08/2018	Matjhabeng ICT		

1. INTRODUCTION

The Matjhabeng IT Department's primary function is to ensure reliable and consistent delivery and support of Information Communication & Technology (ICT) services and/or infrastructure throughout the Municipality, thereby enabling the municipality to optimally execute its mandate. The IT Department therefore continually provides and deploys ICT enabling tools to manage and improve business processes.

As part of becoming more competitive and better supporting the municipality and business priorities, The IT Department has initiated the development of a Disaster Recovery Management Program., thus ensuring business continuity by implementing a Disaster Recovery Plan for mission critical systems.

This DR Strategy and Plan will make provision for resilience against events that could disrupt business as usual activities. The resilience and response approach is to be proportionate to the risk and to a level agreed by the municipality.

2. OBJECTIVES

The objective of this DR Strategy and Plan is to ensure that the risks identified in the Business Impact Analysis (BIA) are mitigated. The analysis focused on critical applications within the municipality. Based on the analysis conducted, the following objectives are targeted:

- Develop capability within the local environment to meet business RTOs and RPOs
- Establish a Disaster Recovery capability at an offsite location for the Head Office server farm.

The diagram below shows a high-level view of the BCM methodology:

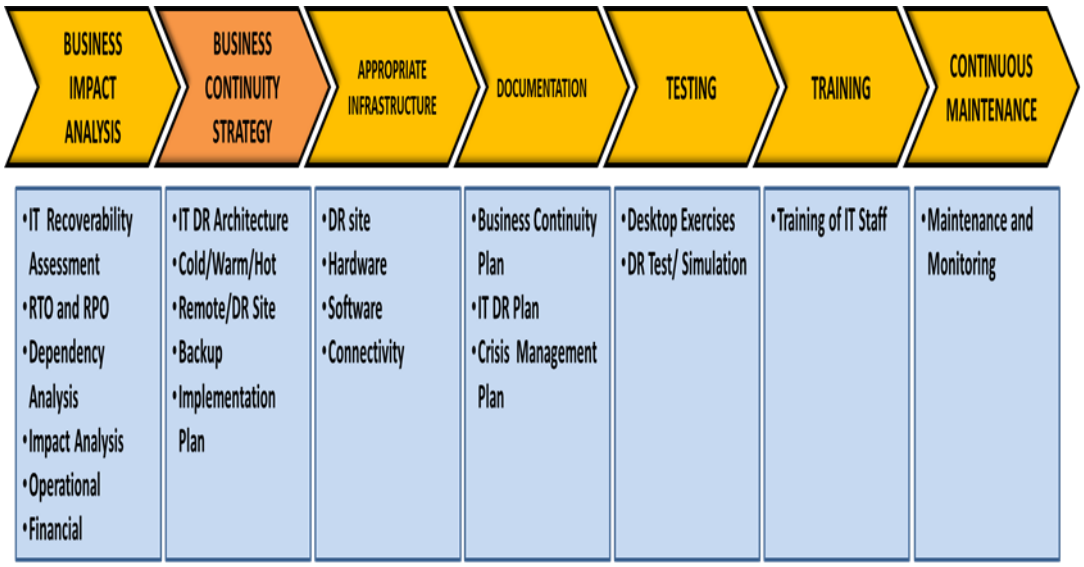


Figure 1: Methodology

3. HIGH LEVEL VIEW OF THE CURRENT STATUS

The municipality has all critical applications and infrastructure hosted at the Head Office Data Centre, 319 Stateway, Welkom. There is a secondary DR site that has been identified in Virginia, 6 Union Street (Main Building), Virginia - however the DR site is not equipped with infrastructure and not yet ready to host any equipment.

The existing environment at the Head Office is not designed to provide a high level of availability - the environment is not adequately resourced to continue normal operations should there be a complete loss of the primary data centre.

The potential data loss could extend to an entire day, and recovery of the entire IT environment at an offsite location from archived backup is untested.

Addressing these shortfalls will contribute towards the achievement of the defined objectives.

The following specific single points of failure have been identified within the current IT environment and must be addressed to achieve the recommended level of resilience:

- Insufficient switch redundancy for servers.
- There are currently no backup servers or clusters in the event of component failures.
- The RTOs and RPOs currently not achieved for critical applications listed in the table below:

RTO	RPO
Solar/ Cash Drawer	Solar/ Cash Drawer
Syntell	Syntell
PayDay	PayDay
MS Office 365	File Sharing/ Local Drives
File Sharing/ Local Drives	
Paperless Agenda	

Table 1: List of applications

4. LEVELS OF RESILIENCE

The level of resilience desired by the municipality will determine the most suitable strategy to be adopted in order to achieve the defined objectives, with the higher the level resulting in an increased ability to meet offsite RTOs and RPOs.

The following levels of resilience are defined, ranked from the lowest level of resilience to the highest:

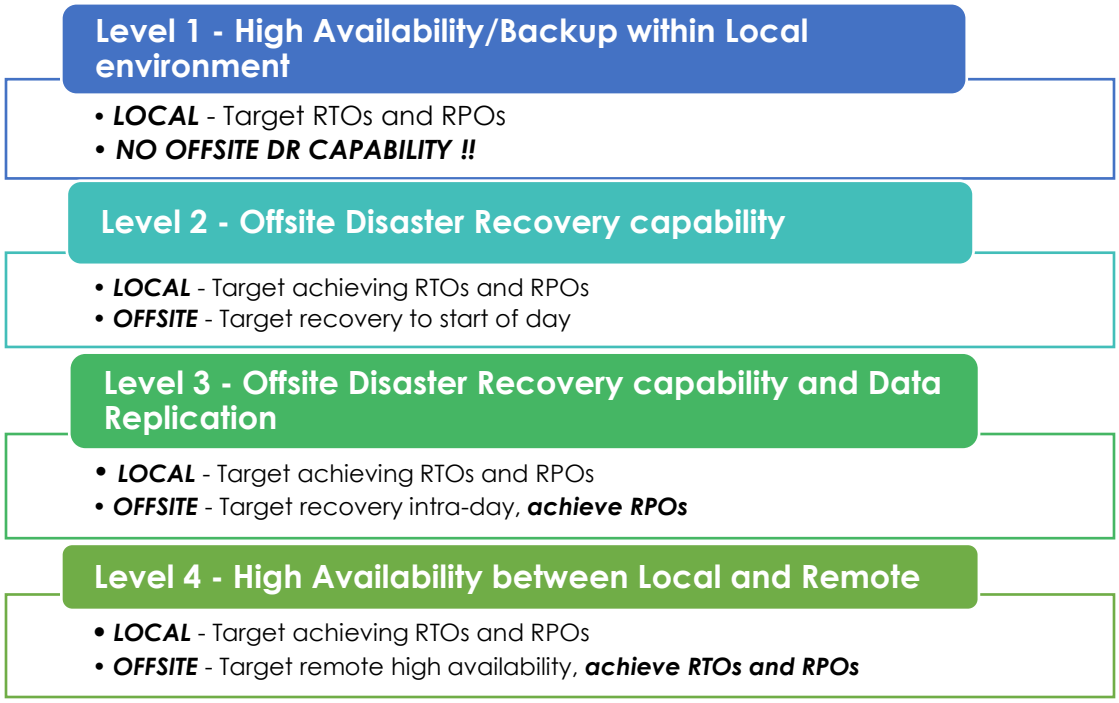


Figure 3: Levels of Resilience

Level 1 is based on shared backup infrastructure and cluster level fail-over in the production environment; no offsite DR capability.

Levels 2-4 include addressing the identified shortfalls within the current environment and level 1 with regards to offsite capability and meeting the required RTO and RPOs.

4.1 RESILIENCE LEVEL RATING

The following table illustrates the rating of the various levels of resilience:

Key	
☺	Good
😐	Average
☹	Bad

	Level 1	Level 2	Level 3	Level 4
Potential data recoverability	☹	😐	😐	☺
Cost	☺	😐	😐	☹
Implementation Time	☺	☺	😐	☹

Table 4: Resilience Level Rating

4.2 TARGET RECOVERY TIMES AND DATA LOSS

The following target recovery times and data loss estimates are associated with each level of resilience at an offsite location:

Level	*Target Recovery Time*	*Potential Data Loss*
Current	Unknown	Unknown
Level 1	Unknown	Unknown
Level 2	48 hours	1 Day
Level 3	Meet RTOs	1 Day
Level 4	Meet RTOs	Meet RPOs

Table 5: Target Recovery

5. RESILIENCE OVERVIEW

Various strategies are proposed in order to attain the desired level of resilience. These levels are not mutually exclusive, and different strategies may be applied to different systems and applications depending on the defined business requirements.

Each level presented comprises the following infrastructural elements:

- Systems – IT server equipment and software
- Storage – Disk hardware and software
- LAN and WAN – Switches, routers
- Telecoms – Remote data centre connectivity
- Data Centre – Computer room space, power and cooling
- Professional Services – Project management, specialist skills

The approach ultimately selected by the municipality is directly dependent on the desired level of resilience.

5.1 LEVEL 1 – HIGH AVAILABILITY/ WARM BACKUP WITHIN EXISTING ENVIRONMENT

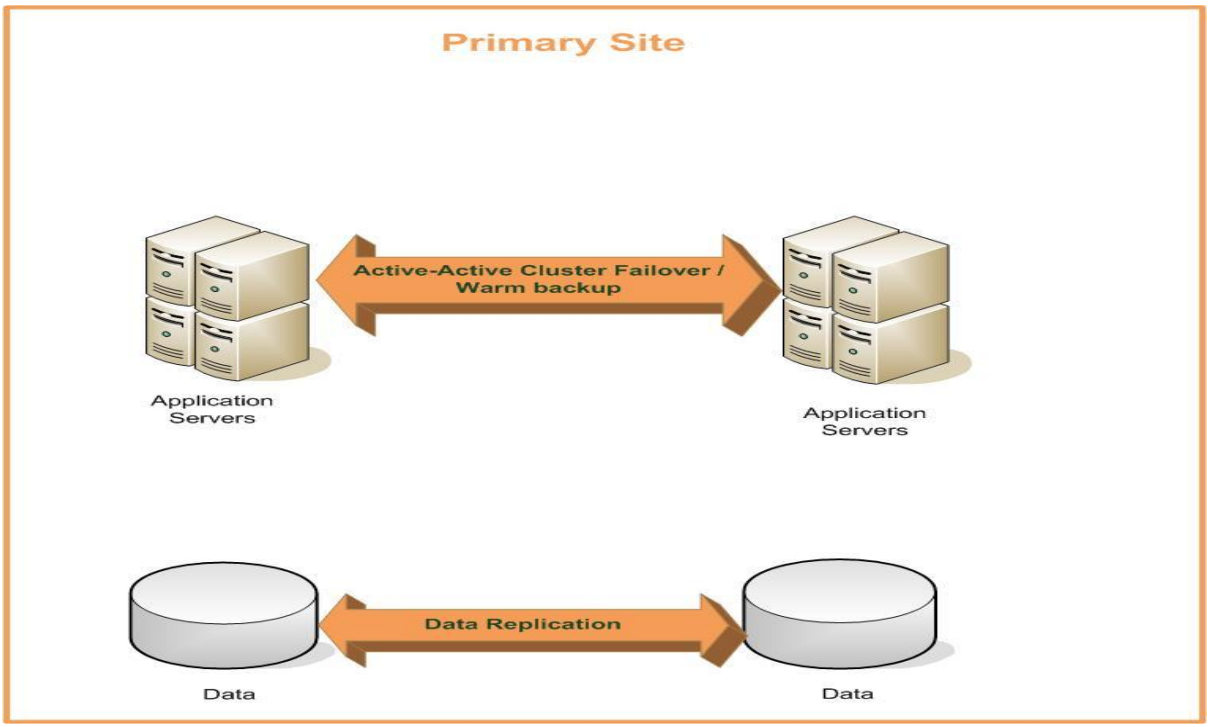


Figure 4: Level 1 Resilience

5.1.1 Overview

This level of resilience is designed to provide a high level of availability, owing to a combination of redundant IT hardware, data replication and software clustering.

This level will not be adequately resourced to continue normal operations following a complete loss of a data centre.

5.1.2 RTO and RPO Targets

Improving the resilience within the existing environment will ensure that business defined RTOs and RPOs can be achieved in the event of component failures, including the applications which are currently at risk mentioned in section 3.

5.1.3 Features

- Fast recovery from an incident affecting a single data centre.
- Improved confidence in ability to fail-over as much of the resilience equipment is being actively used.
- Recovery procedures can be simplified and/or automated, as much of the infrastructure will be up and running.
- Less overhead on change and configuration management as the infrastructure is being continually exercised and so issues are likely to be identified more quickly than where equipment is not be used.
- Live fail-over rehearsals are easier to implement.

5.1.4 Disadvantages

- Insufficient provision is made against total loss of the data centre.
- Data corruption and software bugs can affect both environments.
- Can be more difficult to implement and manage than other models.
- May require additional load balancing technology to split services.
- Complex database and application issues may arise.
- Finding the same hardware to restore to at an alternate site would be mostly impossible as the vendors change models regularly.

5.2 LEVEL 2 – OFFSITE DISASTER RECOVERY CAPABILITY

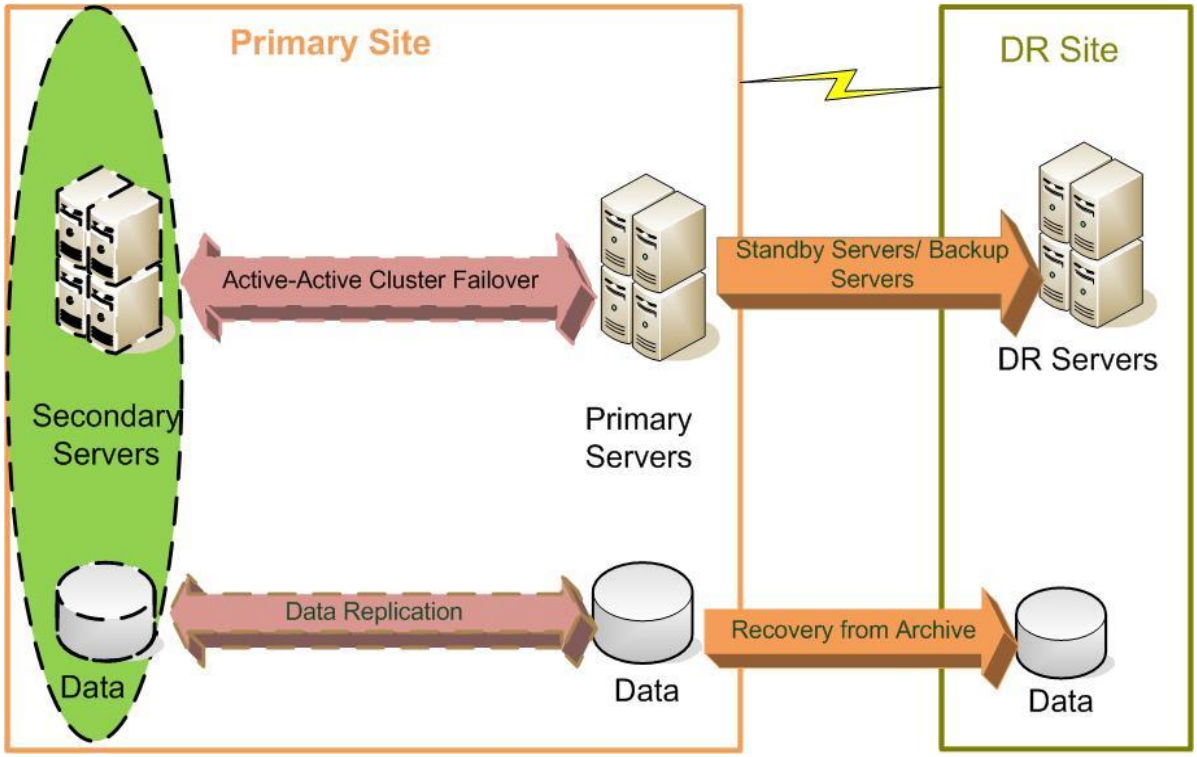


Figure 5: Level 2 Resilience

5.2.1 Overview

This level of resilience provides for an offsite DR capability in order to cater for a worst-case scenario that disables the production data centre. The recovery of systems will be from archived backups to a specific point in time.

Additional IT equipment and infrastructure will be required and could be shared in order to provide a more cost-effective recovery environment. A highly efficient level of change control and regular testing will be required in a syndicated environment.

5.2.2 Approach

This level provides for SAN at an offsite recovery location used for the recovery of data from archived backup.

Dedicated servers are maintained in either a cold or warm state at the remote recovery site, ready for operation in a short space of time.

A high-speed WAN link is recommended for system updates and online backup to the remote recovery centre.

5.2.3 RTO and RPO Targets

Business defined RTOs and RPOs cannot be achieved in the event of a complete failure at the production data centre, however recovery from archived backup will be possible subject to longer recovery timeframes and greater potential data loss.

The potential loss of data could extend to an entire day, as the strategy for this level is based on recovery from the previous night's archived backup.

5.2.4 Features

- Provision is made for a major incident that disables the production data centre.
- Provision of an isolated recovery and test environment.
- Ability to test system recovery to a point in time from archived backup.
- Short timeframe to implement physical environment.

5.2.5 Disadvantages

- Slowest recovery from an incident.
- Lengthy timeframe associated with recovery from backup archive.
- Server and network environment will still need to be manually recovered.
- Change and configuration will require time and resources.
- Maturity in achieving successful recoveries will require regular rehearsals.

5.3 LEVEL 3 – OFFSITE DR CAPABILITY AND DATA REPLICATION

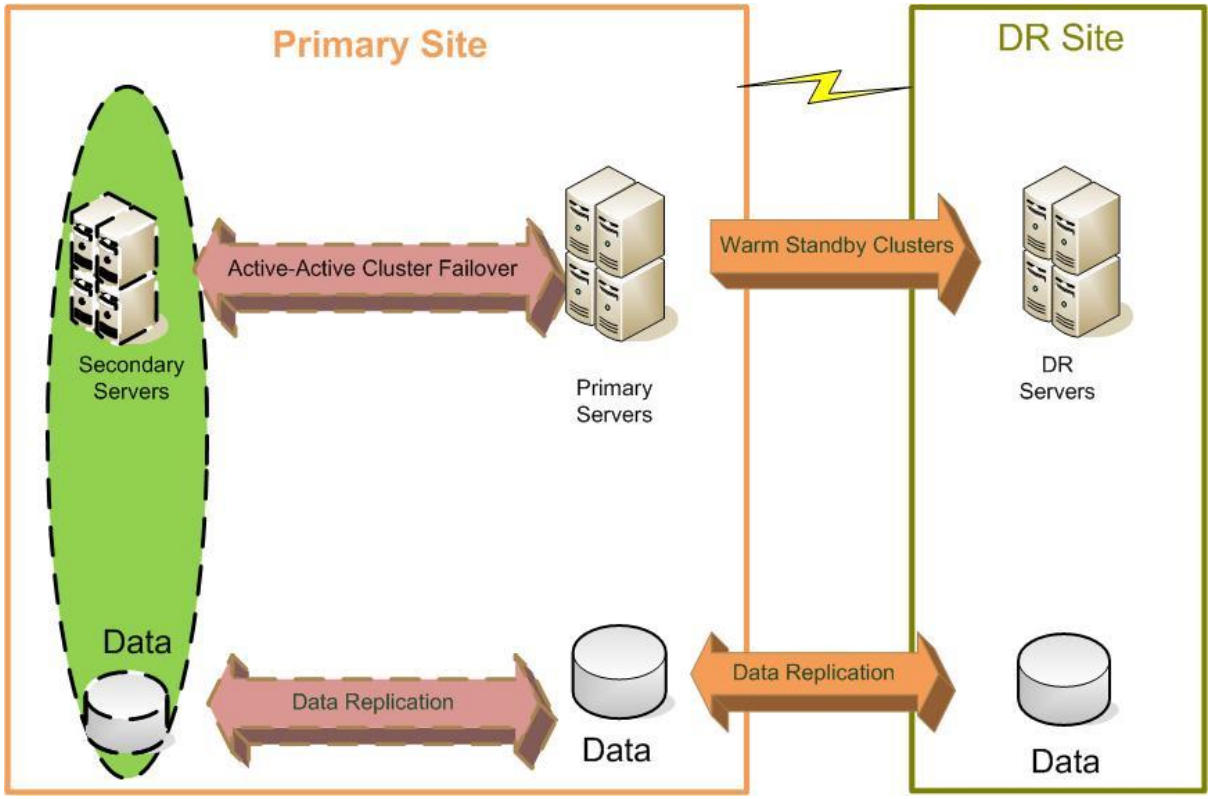


Figure 6: Level 3 Resilience

5.3.1 Overview

This level of resilience provides the municipality with an offsite storage of replicated data (some synchronously) in order to reduce the recovery time in the event of a major incident affecting the production data centre.

Replication of data will require investment in disk storage, replication software and significant bandwidth between the two sites.

5.3.2 Approach

This level provides for high specification SAN at an offsite recovery location used for the replication of data from the production environment.

Dedicated servers are maintained in a warm state at the remote recovery site, ready for operation in a short space of time.

A high-speed WAN link is recommended in order to facilitate data replication and DR system updates.

5.3.3 RTO and RPO Targets

Recovery from replicated disk storage will be possible and RPOs can be achieved.

The potential loss of data may extend to the start of day, as the strategy for this level is based on a worst-case scenario of recovering to a consistent state from the replicated data store.

5.3.4 Features

- All the advantages associated with the high availability environment are retained.
- Provision is made for a major incident that disables the production data centre.
- A copy of data is stored off-site.
- Provision of an isolated recovery and test environment.
- Ability to test recovery to point in time at the remote site.

5.3.5 Disadvantages

- Additional costs associated with a remote site.
- Some manual intervention to facilitate recovery is still required (not seamless).

5.4 LEVEL 4 – HIGH AVAILABILITY BETWEEN LOCAL AND REMOTE SITES

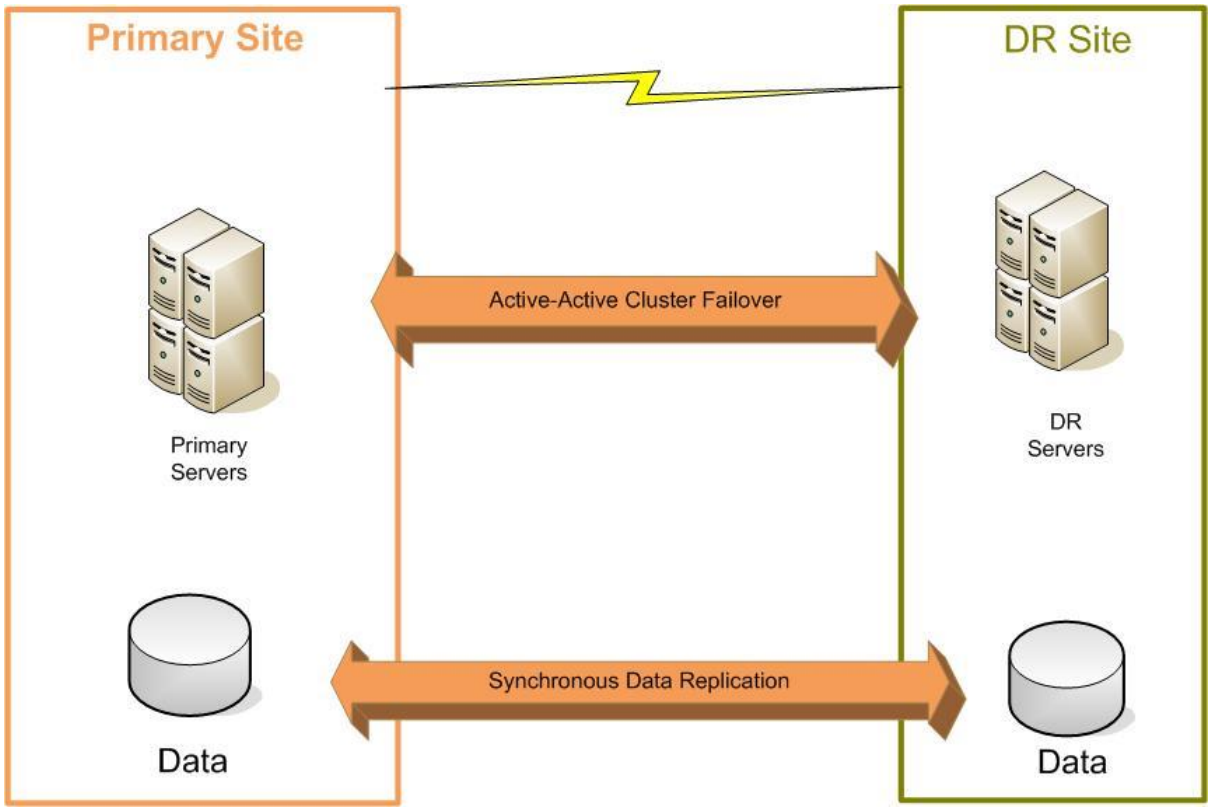


Figure 7: Level 4 resilience

5.4.1 Overview

This level of resilience provides for a remote high availability environment which is situated at a suitable distance from the production data centre.

Consolidation of HA capabilities at the production site could facilitate the transfer of some hardware and infrastructure and additional elements will be required to ensure the elimination of any single points of failure. The most significant cost would be the provision of high capacity, resilient bandwidth between the two sites.

5.4.2 Approach

This level provides for high specification SAN at an offsite recovery location used for the synchronous replication of data from the production environment.

Dedicated servers are clustered remotely with systems able to failover should the Production data centre be disabled.

A high-speed resilient network link is required between the production and remote environments to facilitate data replication, server clustering and processing failover.

5.4.3 RTO and RPO Targets

Business defined RTOs and RPOs can be achieved in the event of an outage affecting the production data centre.

The potential for data loss is eliminated as this level of resilience provides for synchronous data replication and cluster failover between the production and offsite DR locations.

5.4.4 Features

- Fast recovery from an incident
- Improved confidence in ability to fail-over as much of the resilience equipment is being actively used at each site.
- Recovery procedures can be simplified and/or automated, as much of the infrastructure will be up and running.
- May improve utilisation of the infrastructure.
- Less overhead on change and configuration management as sites are being continually exercised and so issues are likely to be identified more quickly than where equipment is not be used.
- Live fail-over rehearsals are easier to implement.

5.4.5 Disadvantages

- Significant cost associated with bandwidth connectivity between sites and relocation of installed infrastructure and equipment.
- Can be more difficult to implement and manage than other models.
- May require additional load balancing technology to allow services to be split across remote sites.
- Complex database and application issues may arise.
- Network latency may be an issue.

6. RECOMMENDED STRATEGY IMPLEMENTATION

The proposed strategy targets the achievement of a hybrid level of resilience for the different applications. This was driven by the input from the business units within the municipality and the applications were matched to the appropriate level of resilience depending on the requirements.

It is recommended that the municipality implement the solution in a phased approach, starting with phase 1 as getting the recovery site in Virginia ready can be a long process. The recommended implementation plan below initially focuses on the solutions that can be implemented in a short period of time to achieve RTO and RPO in the local environment, also with the view of achieving DR capability in the long term.

Levels 3 and 4 of resilience represent an idealistic scenario that should form the basis of a long-term strategy and should be actively considered when planning future production IT strategies. The continued improvement in cost of telecom services, as well as advancements in IT technology, software services and server virtualisation will contribute towards achieving this level of resilience.

Additional human resources and management will be required to develop the skills, processes and plans associated with establishing and maintaining a successful IT service continuity strategy.

6.1.1 Phase 1:

Objective	To achieve high availability for applications with RTO and RPO lower than 8 hours.
Actions	• Upgrade the existing servers e.g. dual network cards, dual power supply, RAID 5 • Upgrade the switching in the data centre to provide redundancy. • Upgrade power and air-conditioning to remove single points of failure. • Establish a redundant point of presence (Link) at the DR site.

- Configure high availability for the applications listed in (a) below.

(a) Applications recommended for this phase

Based on the analysis, the following applications within the municipality are recommended for this phase:

Application	Current Level	Current Location
Solar/ Cash Drawer	Level 1	HO Data Centre
Syntell	Level 1	HO Data Centre
PayDay	Level 1	HO Data Centre
MS Office 365 (Internet Links)	Level 1	HO Data Centre
File Sharing/ Local Drives	Level 1	HO Data Centre
Paperless Agenda (Internet Links)	Level 1	HO Data Centre

Table 6: Level 1 Applications

6.1.2 Phase 2:

Objective

Based on level 2 as described in section 5.2, obtain/prepare a Disaster Recovery site.

Actions

- Acquire a Disaster Recovery site for the Head office.
- Establish DR capability at the Virginia site.
- Acquire necessary hardware for Level 2 resiliency e.g. tape backup infrastructure, servers for DR site.
- Configure servers hosting the applications listed in (a) below for level 2 of resilience.

(a) Applications recommended for this level

Based on the analysis, the following applications within the municipality are recommended for this level:

Application	Current Level	Current Location
Solar/ Cash Drawer	Level 1	HO Data Centre
Syntell	Level 1	HO Data Centre
PayDay	Level 1	HO Data Centre
MS Office 365 (Internet Links)	Level 1	HO Data Centre
File Sharing/ Local Drives	Level 1	HO Data Centre
Paperless Agenda (Internet Links)	Level 1	HO Data Centre

Table 7: Level 2 Applications

6.1.3 Phase 3:

Objective: Transfer the HA/UAT hardware to the DR site to achieve level 3 as described in section 5.3.

Actions:

- Acquire necessary hardware for replication and backup.
- Upgrade the WAN network infrastructure.
- Acquire necessary hardware for Level 3 resiliency e.g. tape backup infrastructure, servers and SAN the for DR site
- Configure servers hosting the applications listed in (a) below for level 3 of resilience.

(a) Applications recommended for this level

Based on the analysis, the following applications within the municipality are recommended for this level:

Application	Current Level	Current Location

Table 8: Level 3 Applications

6.1.4 Phase 4:

Objective: Implement high availability between the sites as described in section 5.4.

Actions:

- Upgrade the WAN network infrastructure to cater for high availability between sites.
- Configure servers hosting the applications listed in (a) below for level 4 of resilience.
- Move the servers configured for high availability in level 1 to the DR site.

(a) Applications recommended for this level

Based on the analysis, the following applications within the municipality are recommended for this level:

Application	Current Level	Location

Table 9: Level 4 Applications

6.2 TELECOMMUNICATIONS

6.2.1 Connectivity to Telkom

6.2.2 Connectivity to Remote Sites (Telkom VPN)

6.3 GENERAL RECOMMENDATIONS

- It is recommended that the municipality develop business continuity plans for the different business units – This IT DR Strategy and Plan will be the subset of the overall business continuity plan.
- It is recommended that the municipality perform Disaster Recovery tests annually to validate that the DR hardware implemented meets the business requirements.
- The backup strategy must be revisited, and the municipality must consider offsite storage of the backup tapes.
- Single points of failure must be addressed within the current environment; addressing these shortfalls will contribute towards the achievement of the defined objectives.
- The detailed design of this solution should take virtualisation and data lifecycle management into consideration in order to provide a resilient and manageable environment in which to fail over processing or recover systems to a specific point in time.
- The production server room must be supported by UPSs and generator electricity to maintain systems in a power outage – the room must also be supported by adequate air-cooling systems.
- The municipality must ensure that all servers are hosted in the dedicated data centre and not scattered in the office environments.

6.4 BEST PRACTICE

The following standards and codes of practice are referenced in suggesting a long term strategy:

6.5 *ISO 24762*

"DR sites should be in geographic areas that are unlikely to be affected by the same disaster/failure events as organizations' primary sites. The issue of site proximity and associated risks should be taken into consideration when ICT DR service providers contract and agree SLAs with organizations."

6.6 *The PAS77: 2006 IT Service Continuity Management Code of Practice*

"Location and distance between sites: If failing over from one site to another the network path distance between the two sites should be carefully considered. If the two sites are too close together, for example on a campus, they could be impacted by the same natural disaster. If too far apart then the cost of connecting the two sites with suitable telecommunications and/or courier services could become prohibitive. Most importantly the distance between the sites could have a negative impact on the way in which the IT systems operate. If the chosen model includes synchronous replication, then the greater the distance the greater the latency, thus introducing delays in the transfer of data between sites which could in turn impact application performance."

"Business Continuity Management (BCM) is concerned with managing risks to ensure that at all times an organization can continue operating to, at least, a pre-determined minimum level."

7. 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 DR Strategy	Date
Executive Director: SSS, who hereby recommends and approves this DR Strategy	Date
Acting ICT Manager: who hereby recommends this DR Strategy	Date

Information Communication and Technology (ICT)

Matjhabeng Local Municipality

(MLM)

IT Continuity Plan

Document Version: 1.0 (Draft)

POLICY DOCUMENT CONTROL PAGE

Document Number	ICT Continuity Plan v1.0

ORIGINATOR

Custodian	ICT Department
Responsible Person	IT Manager

APPROVAL

Approval date by Legal Services	
Approval date by Risk	
Approval date by ICT Steering Committee	
Approval date by Council	

CIRCULATION

Effective Date	
Circulated by	Pulane Rakotsoane

POLICY REVIEW

Recommended Review Period	Every 3 years

This plan has been endorsed by the Matjhabeng Local Municipality IT Manager:

_____

Pulane Rakotsoane

IT Manager DATE: ____/____/____

This plan has been endorsed by the Matjhabeng Local Municipality Municipal Manager:

_____

Thabiso Tsoaeli

Municipal Manager DATE: ____/____/____

Table of Contents

1.1 EXECUTIVE SUMMARY

Planning for the Matjhabeng Local Municipality in the aftermath of a disaster is a complex task. Preparation for, response to, and recovery from a disaster affecting the operations of the department(s) requires the cooperative efforts of many stakeholders in partnership with the functional areas supporting the "business" of the Municipality.

This Document records the ICT recovery plan (DRP) indicating the steps to be taken to recover critical IT infrastructure.

Should the IT Systems encounter a disaster that prevents them from functioning, The IT Department and IT Service providers should be prepared to provide adequate computational data storage and data communications services and facilities at an off-site disaster recovery source for the participating applications.

The offsite Disaster Recovery Resource is a fully operational data centre that is prepared to host the critical systems such as Cash Drawer, File Sharing, Syntell, Solar, Telephony, PayDay, Paperless Agenda, Microsoft End User Computing (EUC) and MS Office 365 and Email.

1.2 HOW TO USE THIS DOCUMENT

Use this document for

- Recovering critical IT infrastructure from a disaster
- Planning for the continuity of the critical and essential business functions at the Municipality.
- As a checklist of preparation tasks.
- For training personnel.

1.3 PURPOSE

This Disaster Recovery Plan establishes procedures to recover the Matjhabeng Local Municipality systems following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
  - **Notification Phase** to detect interruption and alert.
  - **Activation phase** to assess damage and to activate the plan.
  - **Recovery phase** to restore temporary ICT operations and recover damage done to the original system.
  - **Reconstitution phase** to restore ICT system processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out Municipal systems processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated Municipal personnel and provide guidance for recovering systems during prolonged periods of interruption to normal operations.
- Ensure coordination with other Municipal staff who will participate in the Disaster Recovery planning strategies.
- Ensure coordination with external points of contact and vendors who will participate in the Disaster Recovery planning strategies.

1.4 APPLICABILITY

The Matjhabeng Local Municipality Disaster Recovery Plan applies to the functions, operations and resources necessary to restore and resume ICT systems operations. The Disaster Recovery Plan applies to Matjhabeng Local

Municipality and all other persons associated with Matjhabeng Local Municipality ICT systems as identified under Section 3, Roles and Responsibilities.

1.5 SCOPE

The ICT continuity plan is aimed at restoring Matjhabeng Local Municipality critical ICT systems to enable business to continue to operate after a disaster has rendered any or all the systems inoperable.

2. AUDIENCE

The Disaster Recovery Champions and the associated teams responsible for ICT and security at system and operational levels can use the principles presented in this document. This description includes the following personnel:

- Management team responsible for overseeing ICT operations or business processes that rely on ICT systems.
- System administrators responsible for maintaining daily ICT operations
- Information System Security Officers (ISSOs) and other staff responsible for developing, implementing, and maintaining an organization's ICT security activities
- System engineers and architects responsible for designing, implementing, or modifying information systems.
- Users who employ desktop and portable systems to perform their assigned job functions
- Other personnel responsible for designing, managing, operating, maintaining, or using information systems.

In addition, emergency management personnel who may need to coordinate facility-level contingency may use this document with ICT Disaster Recovery Planning activities.

3. ICT MISSION CRITICAL SYSTEMS

The following ICT provided services are important for the Matjhabeng Local Municipality's daily operations

- Cash Drawer
- Syntell
- Solar
- PayDay
- Paperless Agenda

The following ICT provided services are essential but not critical for the Matjhabeng Local Municipality's daily operations:

- Office 365 and Email
- Internet and Intranet
- Computer Equipment
- Telephony,

The details of these systems, including Vendor, Functionality and Location are found in ***Appendix B.***

4. DRP TEAMS & RESPONSIBILITIES

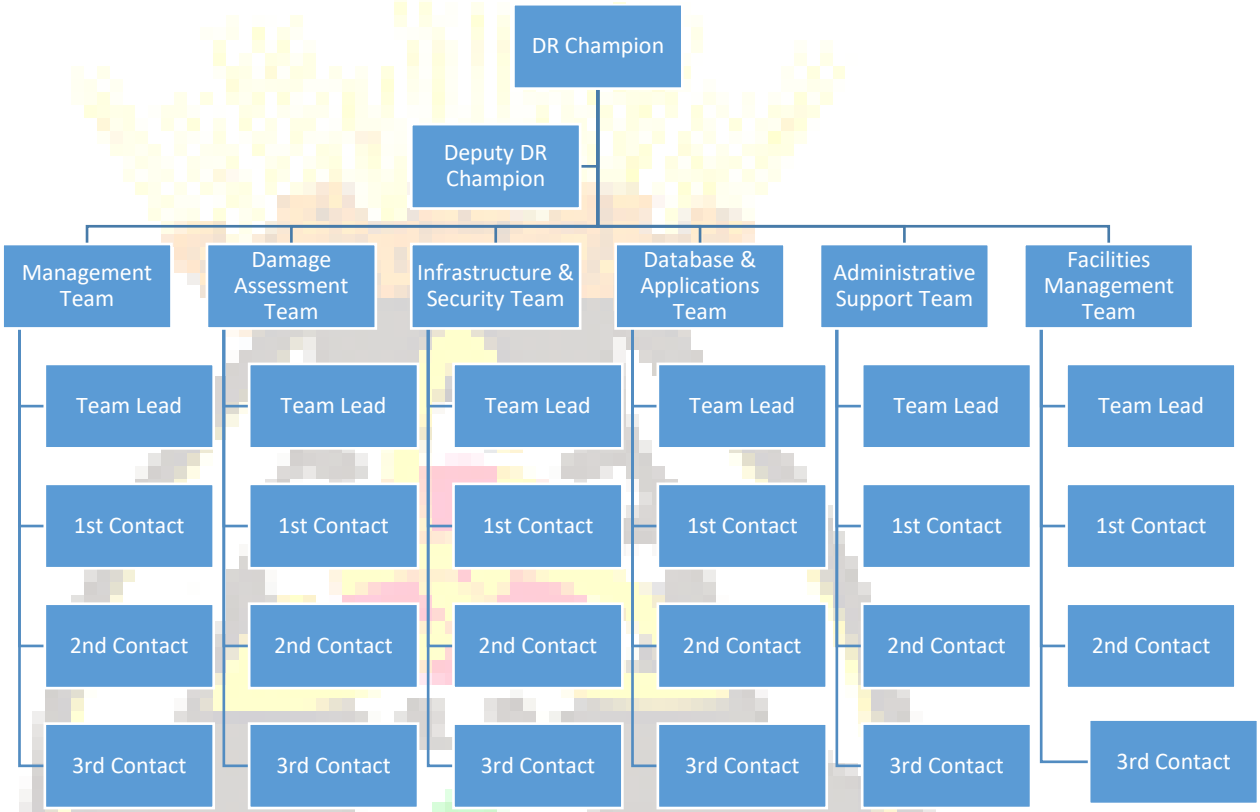
The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery.

The following teams have been developed and trained to respond to a Disaster event affecting the ICT system. Disaster Recovery Plan establishes several teams assigned to participate in recovering Matjhabeng Local Municipality system operations.

- DRP Champion
- DRP Management Team
- DRP Damage Assessment Team
- Server and LAN Recovery Team
- Database & Applications Recovery Team
- Hardware Salvage Team
- Security (IT & Physical) Team
- Telecommunications & WAN Recovery Team
- Alternate Site Recovery Coordination Team
- Original Site Restoration/Salvage Coordination Team
- Test Team
- Communications & Administrative Support Team
- Procurement Team (Equipment & Supplies) Team

All the teams above will work together under the supervision of the DRP Champion and the Management team and all will be responsible for recovery of the Matjhabeng Local Municipality computer systems environment and all applications. Members of the DRP teams include personnel who are also responsible for the daily operations and maintenance of Matjhabeng Local Municipality systems. The Damage Assessment team leader directs the DRP team. Teams, information details, roles and responsibilities are described in ***Appendix F***

Below is depiction various DRP teams organogram.



5. NOTIFICATION AND ACTIVATION PHASE

The Notification/Activation Phase defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, assess system damage, and implement the plan. At the completion of the Notification/Activation Phase, recovery staff will be prepared to perform contingency measures to restore system functions on a temporary basis.

5.1 NOTIFICATION PROCESS

The notification sequence is listed below:

- The first responder is to notify the Disaster Recovery Planning Champion.
- All known information must be relayed to the Disaster Recovery Planning Champion.

- The Disaster Recovery Planning Champion will instruct the Damage Assessment Team Leader to begin assessment procedures.
- The Damage Assessment Team Leader is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time.

More notification procedures defining this phase are described in ***Appendix C.***

5.2 DAMAGE ASSESSMENT PROCESS

The Damage Assessment Team assesses and determines the following:

- Cause of the emergency or disruption and potential for additional damage;
- Status of physical infrastructure such as structural integrity of computer room, condition of electric power, telecommunications, and heating, ventilation, and air-conditioning
- Inventory and functional status of ICT equipment such as fully functional, partially functional, and non-functional
- Type of damage to ICT equipment or data such as water damage, fire and heat, physical impact, and electrical surge
- Items to be replaced such as hardware, software, firmware, and supporting materials
- Once the impact to the system has been determined, the appropriate teams will be notified of updated information and planned response to the situation.
- Notifications will be executed using the procedures described in ***Appendix G***
- The Damage Assessment team will personally visit the site and make an initial determination of the extent of the damage. Based on their assessment, all or part of the Disaster Recovery Plan will be initiated. The team will decide:
- If the action plan requires the assistance of other recovery team members, those team members will be notified.

6. PLAN ACTIVATION PHASE

The Disaster Recovery Plan should be activated only when the damage assessment indicates that one or more of the activation criteria for that system are met. If an activation criterion is met, the Disaster Recovery Champion will activate the plan.

Plan and Activation phase will be executed using the procedures described in ***Appendix C.***

6. RECOVERY PHASE

Recovery operations begin after the contingency plan has been activated, damage assessment has been completed (if possible), personnel have been notified, and appropriate teams have been mobilized.

Recovery phase activities focus on contingency measures to execute temporary ICT processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility.

At the completion of the Recovery Phase, the ICT system will be operational and performing the functions designated in the plans. All the plans for operations in the recovery site are documented in ***Appendix G.***

6.1 RECOVERY PROCESS

Procedures assigned to the appropriate recovery team address the following actions:

- Obtaining authorization to access damaged facilities
- Notifying internal and external business associated with the system
- Obtaining necessary office supplies and work space
- Obtaining and installing necessary hardware components
- Obtaining and loading backup media
- Restoring critical operating system and application software
- Restoring system data
- Testing system functionality including security controls

- Connecting system to network or other external systems
- Obtaining user acceptance

The sequence of recovery activities are documented in the plans found in ***Appendix G***

7. RECONSTITUTION PHASE

In the reconstitution phase, operations are transferred back to the facility once it is free from the disaster after effects, and execution phase activities are subsequently shut down. If the original system or facility is unrecoverable, this phase also involves rebuilding. Hence the reconstitution phase can last for a few days to a few weeks or even months, depending on the severity of the destruction and the site's fitness for restoration.

The following major activities occur in this phase:

- Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental controls, office equipment, and supplies
- Installing system hardware, software, and firmware. This activity includes detailed restoration procedures as documented in the Recovery Phase
- Establishing connectivity and interfaces with network components and external systems
- Testing system operations to ensure full functionality
- Backing up operational data on the contingency system and uploading to restored system
- Shutting down the contingency system
- Terminating contingency operations
- Securing, removing, and/or relocating all sensitive materials at the contingency site
- Arranging for recovery personnel to return to the original facility.

Reconstitution phase will be executed using the procedures described in ***Appendix H.***

8. POST DISASTER RECOVERY REVIEW

Two debriefings are schedule on the days immediately following the hot site test. One is for the Team participants to assess the systems software recovery procedures. The second is for the user community who participated in the recovery.
These meetings are general discussions to address:

- Areas where the exercise was successful;
- Problems that were encountered; and
- Suggestions for improvements.

Based on the conclusions, an action list of improvements to be made prior to the next test is developed and responsibility for implementing them is assigned
Post Disaster Recovery Review phase will be executed using the procedures described in ***Appendix H.***

9. TESTING THE DISASTER RECOVERY PLAN

The Matjhabeng Local Municipality ICT Disaster Recovery plan is tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The test provides an opportunity to identify any omissions in recovery procedures or documentation and to determine whether personnel are adequately prepared to perform their assigned duties. Therefore, IT regularly schedules exercises of its disaster recovery plan at the Recovery Site. The following areas are addressed in the Disaster Recovery test:

- Readiness of Disaster recovery site
- System recovery on an alternate platform from backup media
- Coordination among recovery teams (including service providers)
- Internal and external connectivity
- System performance using alternate equipment and support teams
- Restoration of normal operations
- Notification procedures.

Testing the Disaster Recovery Review Plan will be executed using the procedures described in ***Appendix I.***

8 TRAINING AND AWARENESS

In addition to regular test, team members, managers and support team receive annual refresher training regarding the emergency alert procedures.

Recovery personnel will be trained on the following plan elements:

- Purpose of the plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements
- Team-specific processes (Notification, Damage Assessment, Activation, Recovery, and Reconstitution Phases)
- Individual responsibilities (Notification, Damage Assessment, Activation, Recovery, and Reconstitution Phases).

All other users are provided with appropriate disaster recovery awareness information.

9 PLAN MAINTENANCE

The Disaster Recovery Champion is responsible for the maintenance of this document. The Disaster Recovery Plan need to be kept up to date with the current organisation environment.

Matjhabeng Local Municipality plan will be reviewed for accuracy and completeness annually. At a minimum, the plan reviews will focus on the following elements:

- Operational requirements

- Security requirements
- Technical procedures
- Hardware, software, and other equipment (types, specifications, and amount)
- Names and contact information of team members
- Names and contact information of vendors, including alternates
- Alternate and offsite facility requirements
- Vital records (electronic and hardcopy).

Additionally, the plan will be updated in the event an actual disaster occurs. The plan will be reviewed and updated at a convenient point after initial responses to the disaster have been completed.

10 PLAN APPENDICES

The appendices provide key details not contained in the main body of this plan. The appendices associated with this document are:

Appendix A: GLOSSARY OF TERMS

Appendix B: LIST OF ICT MISSION CRITICAL SYSTEMS

Appendix C: SPECIFIC TECHNICAL, OPERATIONS AND MANAGEMENT REQUIREMENTS

Appendix D: EMERGENCY CONTACT NUMBERS

Appendix E: CRITICAL SYSTEM PROCESSING INFORMATION

Appendix F: DISASTER RECOVERY SUPPORT TEAMS

Appendix G: DAMAGE ASSESSMENT PROCEDURES

Appendix H: RECOVERY SITE OPERATION PROCEDURES

Appendix I: DRP RECOVERY GUIDES

Information Communication and Technology (ICT) Firewall Policy

Matjhabeng Local Municipality

(MLM)

Table of Contents

1. INTRODUCTION

Information and systems security have become increasingly important to the municipality driven by technological changes and current and new regulatory changes. Information security is one of the main issues in the current municipality ICT infrastructure and IT systems. The Firewall is one of the key parameters gatekeepers in the IT Security and infrastructure that maintains and up hold the integrity of IT systems.

2. SCOPE

This policy applies to all Firewalls within the MLM. This is managed either by third parties or by internal assigned IT professionals. Deviations from this policy will be done in accordance to Policy, in writing and authorised by the ICT Manager. All MLM systems playing the role of firewalls, whether they are formally called firewalls, must be managed according to the rules defined in this policy. In some instances, this will require that these systems be upgraded so that they support the minimum functionality defined in this policy.

3. REQUIREMENTS

Prior to deployment of any Firewall at and MLM offices there has to be a diagram reflecting the permissions' path. This will also consist of the jurisdiction on each on these pathways, a description of each pathway, and must be submitted to the ICT manager. This is also the training to the level of administrators of the PaloAlto to a competent level to manage the system within the confines of the MLM council.

4. TECHNICAL EDUCATION

Members that administer the firewall system must be a competent level of understanding and education in order to manage and run the administrative roles required in this position.

5. DEFAULT AND DENIAL

Every connectivity path and service that is not specifically permitted by this policy and supporting documents issued by the ICT department must be blocked by MLW firewalls.

The list of currently approved paths and services

- Must be documented and distributed to all system administrators with a need to know by the ICT department.
- The IT department must maintain an inventory of all access paths in and out of MLM internal networks.

6. CONNECTIONS BETWEEN MACHINES

Real-time shared connections between two or more MLM computer systems must not be established or enabled unless the ICT department has determined that such connections will not jeopardize information security and must be filtered through the Firewall. This requirement applies no matter what technology is used, including wireless connections, microwave links, cable modems, integrated services digital network lines, and digital subscriber line connections. Any connection between an in-house MLM production system and any external computer system, or any external computer network or service provider, must be approved in advance by the ICT department.

7. REGULAR TESTING

Because firewalls provide such an important control measure for MLM networks, their strength and proper configuration must be tested on a regular basis. Where vendor software supports it, this testing must include the use of software agents that automatically check to determine whether firewalls remain configured and running in a manner that is consistent with both MLM security policies and the MLM Information Architectural plan. The vendor has to also provide the training for the skills required to administer the system. This testing process must include consideration of defined configuration parameters, enabled services, permitted connectivity paths, current administrative practices, and adequacy of the deployed security measures, bypass processes. These tests must include the regular execution of vulnerability identification software and the regular performance of penetration tests. These tests must be performed by technically proficient persons, either in the ICT department or working for a third-party contractor. Those responsible for either the administration or management of the involved firewalls must not perform these tests.

8. LOGS

All changes to firewall configuration parameters, enabled services, and permitted connectivity paths must be logged. All suspicious activity that might be an indication of either unauthorized usage or an attempt to compromise security measures also must be logged. His integrity of these logs must be protected with checksums, digital signatures, encryption, or similar measures. These logs must be promptly removed from the recording systems and stored in a physically protected container for at least six months after the time they were recorded. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

9. INTRUSION DETECTION

All MLM firewalls must include intrusion detection systems approved by the ICT department. Each of these intrusion detection systems must be configured according to the specifications defined by the ICT department. Among other potential problems, these intrusion detection systems must detect unauthorized modifications to firewall system files, and detect denial of service attacks in progress. Such intrusion detection systems must also immediately notify by pager the Technical staff that is in a position to take corrective action. All technical staff working on firewalls must be provided with remote access systems and privileges so that they can immediately respond to these incidents even when they are physically removed from the firewall.

10. CONTINGENCY PLANNING

The plans must be periodically tested to ensure that they will be effective in restoring a secure and reliable networking environment. Administrative staff members working on firewalls must prepare and obtain ICT Management approval for contingency plans that address the actions to be taken in the event of various problems including system compromise, system malfunction, system crash, system overload, and Internet service provider unavailability. These contingency plans must be kept current to reflect changes in the MLM information systems environment.

11. EXTERNAL CONNECTIONS

All in-bound real-time Internet connections to MLM internal networks or multi-user computer systems must pass through a firewall before users can reach a logon banner. The computer systems requiring firewall protection include web servers, electronic commerce servers, and mail servers. All personal computers with digital subscriber line or cable modem connectivity must employ a firewall approved by the ICT department. Wherever a firewall supports it, logon screens must have a notice indicating that the system may be accessed only by authorized users, users who log on represent that they are authorized to do so, unauthorized system usage or abuse is subject to disciplinary action including criminal prosecution, and system usage will be monitored and logged. No MLM computer system (This includes personal computers) may be attached to the Internet unless it is protected by a firewall

12. FIREWALL ACCESS PRIVILEGES

Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to a few technically trained individuals with a business need for these same privileges. Unless permission from the ICT Manager has been obtained, these privileges must be granted only to individuals who are full-time permanent employees of MLM, and not to temporaries, contractors, consultants, or outsourcing personnel. All firewalls must have at least two staff members who are adequately trained to make changes, as circumstances require. Such training includes periodic refresher training course or conference attendance to permit these staff members to stay current with the latest developments in firewall technology and firewall operations. Care must be taken to schedule out-of-town ones so that at least one person capable of effectively administering the firewall is readily available at all times. In the event that a third party vendor/service provider is present then the said party will work/abide by the policy set out by MLM.

13. SECURED SUBNETS

Portions of the MLM internal network that contain sensitive or valuable information, such as the computers used by the Human Resources department, should employ a secured subnet. Access to this and other subnets should be restricted with firewalls and other access control measures. Based on periodic risk assessments, the ICT department will define the secured subnets required in the Information Architecture.

14. FIREWALL PHYSICAL SECURITY

All MLM firewalls must be located in locked rooms accessible only to those who perform authorised firewall management and maintenance tasks approved by the ICT Manager. The placement of firewalls in an open area within a general-purpose data processing center is

prohibited, although placement within separately locked rooms or areas, which themselves are within a general data processing center is acceptable. These rooms must be equipped with alarms and an automated log of all persons who gain entry to the room.

15. DEMILITARIZED ZONES

All Internet commerce servers including payment servers, database servers, and web servers must be protected by firewalls, and be located within a demilitarized zone (DMZ), a subnet that is protected from the Internet by one or more firewalls. An internal network, such as an intranet, is also protected from the DMZ subnet by one or more firewalls.

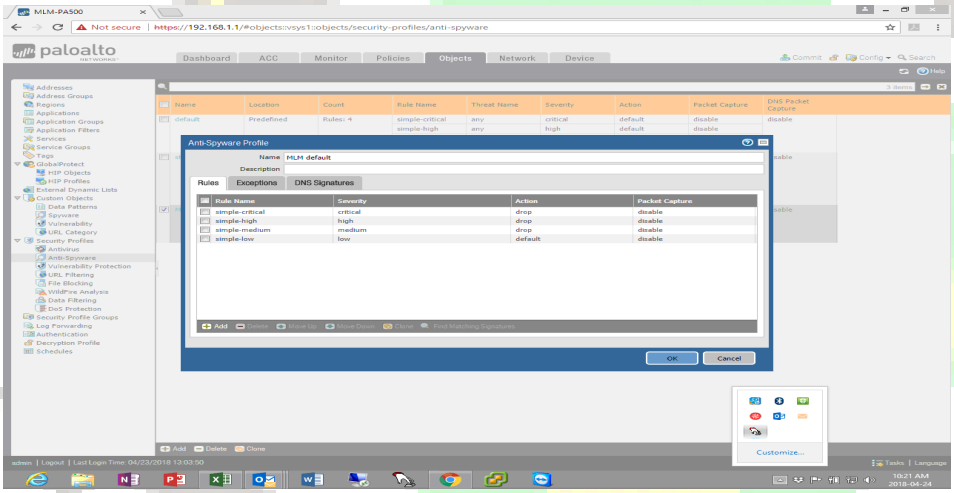
16. NETWORK MANAGEMENT SYSTEMS

Firewalls must be configured so that they are visible to internal network management systems. Firewalls also must be configured so that they permit the use of remote automatic auditing tools to be used by authorized MLM staff members. Unless deliberately intended as a test, such automatic auditing tools must not trigger a response sequence through firewall-connected intrusion detection systems.

17. DISCLOSURE OF INTERNAL NETWORK INFORMATION

The internal system addresses, configurations, products deployed, and related system design information for MLM networked computer systems must be restricted such that both systems and users outside the MLM internal network cannot access this information.

MLM Predefined Anti Spyware



18. SECURE BACKUP

A permissible alternative to offline copies involves online encrypted versions of these same files. Where systems software permits it, the automatic establishment of approved copies of these systems files must proceed whenever an unauthorized modification to these files has been detected. Current offline back-up copies of firewall configuration files, connectivity permission

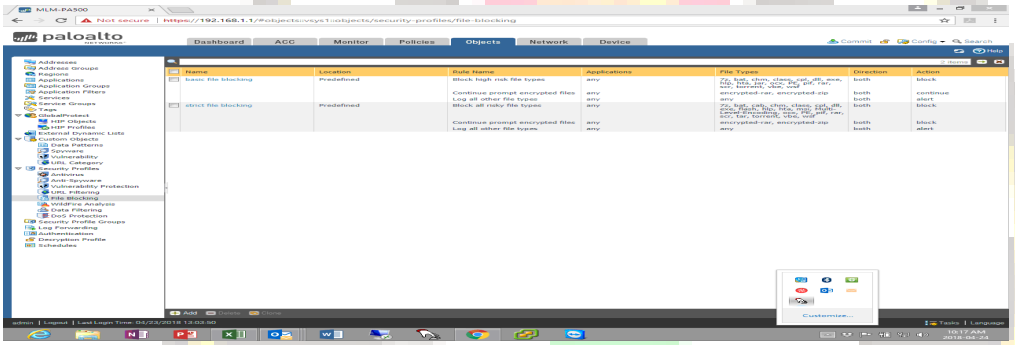
files, firewall systems administration procedural documentation files, and related files must be kept close to the firewall at all times.

19. VIRUS SCREENING AND CONTENT SCREENING

Virus screening software approved by the ICT department must be installed and enabled on all MLM firewalls. Because the files passing through a firewall may be encrypted or compressed, firewall based virus detection systems may not detect all virus-infected files. For this reason, virus screening software is also required at all MLM mail servers, departmental servers, and desktop personal computers. Both content screening software and software that blocks users from accessing certain non-business web sites must also be enabled on all MLM firewalls.

MLM File blocking is currently set as:

Predefined basic and strict file blocking.

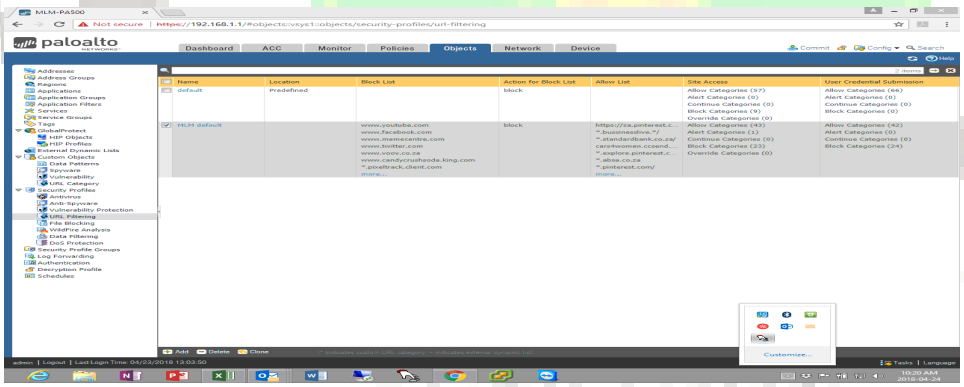


Objects and sites blocking, include

- Video Streaming (You tube note that the SSL is not blocked)
- Social Media(Twitter, Facebook, Memecenter, Voov)

Objects and sites Allowed, include

- Banking sites (Standard Bank, Nedbank, First National Bank, ABSA)
- Business informative and News
- Pinterest (Needs to be assessed for current usage)



20. VIRTUAL PRIVATE NETWORKS

To prevent unauthorized disclosure of sensitive and valuable information, all inbound traffic, with the exception of Internet mail, approved news services, and push broadcasts, that accesses MLM networks must be encrypted with the products approved by the ICT department. These connections are often called virtual private networks (VPNs). The VPNs permissible on MLM networks combine extended user authentication functionality with communications encryption functionality.

21. FIREWALL DEDICATED FUNCTIONALITY

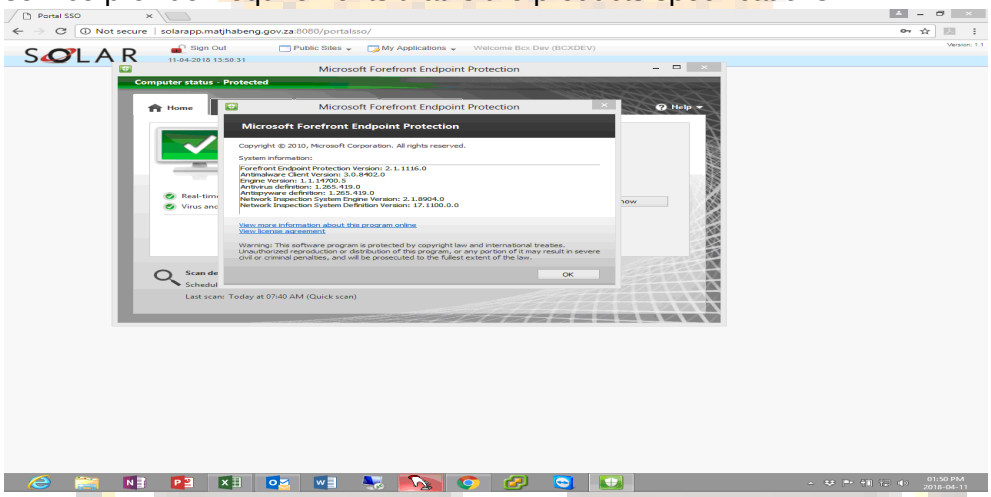
Firewalls must run on dedicated machines that perform no other services, such as acting as a mail server. Sensitive or critical MLM information must never be stored on a firewall. Such information may be held in buffers as it passes through a firewall. Firewalls must have only the bare minimum of operating systems software resident and enabled on them. Where the supporting operating system permits it, all unnecessary and unused systems software must be removed from firewalls. MLM does not permit its internal information to be resident on or processed by any firewall, server, or other computer that is shared with another organization at an outsourcing facility. Outsourcing organization provided shared routers, hubs, modems, and other network components are permissible.

22. FIREWALL CHANGE CONTROL

Because they support critical MLM information systems activities, firewalls are considered all production systems. All changes to the firewall software provided by vendors, excluding vendor-provided upgrades and patches and fixes must go through the Change Management Process. A firewall policy, defining permitted and denied services and connections, should be documented and reviewed at least twice a year by the Security Engineer. Major changes to the MLM internal networking environment, any changes to the production business applications supported, and any major information security incident must trigger an additional and immediate review of the firewall policy. The same documentation that is required for changes on production systems must also be prepared for firewall changes.

23. POSTING UPDATES

MLM firewalls must be running the latest release of software to repel these attacks. Where available from the involved vendor, all MLM firewalls must subscribe to software maintenance and software update services. Unless approved in advance by the ICT Manager, staff members responsible for managing firewalls must install and run these updates within two business days of receipt. As per image below all firewalls within the MLM must be update on a regular basis as per the service provider requirements that is the products specifications.



24. MONITORING VULNERABILITIES

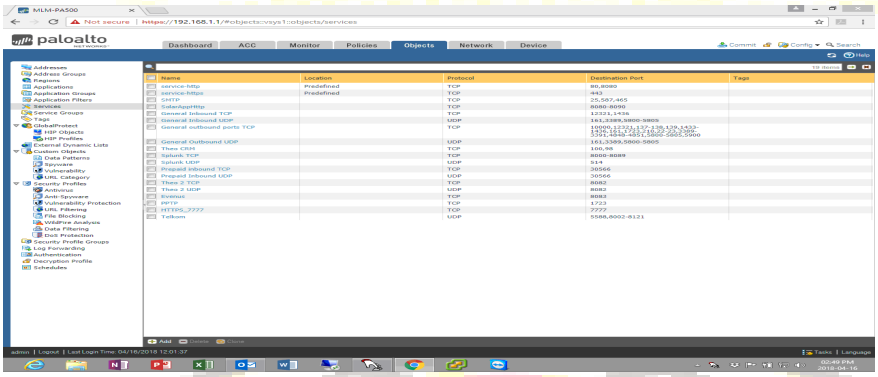
MLM staff members responsible for managing firewalls should stay current with information about firewall vulnerabilities. Any vulnerability that appears to affect MLM networks and systems must promptly be brought to the attention of the ICT Manager.

Part of the vulnerabilities is the ports currently in use. Ports for example 443, 8080. Common ports, such as TCP port 80 (HTTP), may be locked down but other ports may get overlooked and be vulnerable to hackers. In your security tests, be sure to check these commonly hacked TCP and UDP ports: Note that there is software available for PORT vulnerability testing.

- TCP port 21 — FTP (File Transfer Protocol)
- TCP port 22 — SSH (Secure Shell)
- TCP port 23 — Telnet
- TCP port 25 — SMTP (Simple Mail Transfer Protocol)
- TCP and UDP port 53 — DNS (Domain Name System)
- TCP port 443 — HTTP (Hypertext Transport Protocol) and HTTPS (HTTP over SSL)
- TCP port 110 — POP3 (Post Office Protocol version 3)
- TCP and UDP port 135 — Windows RPC
- TCP and UDP ports 137–139 — Windows NetBIOS over TCP/IP

- TCP port 1433 and UDP port 1434 — Microsoft SQL Server

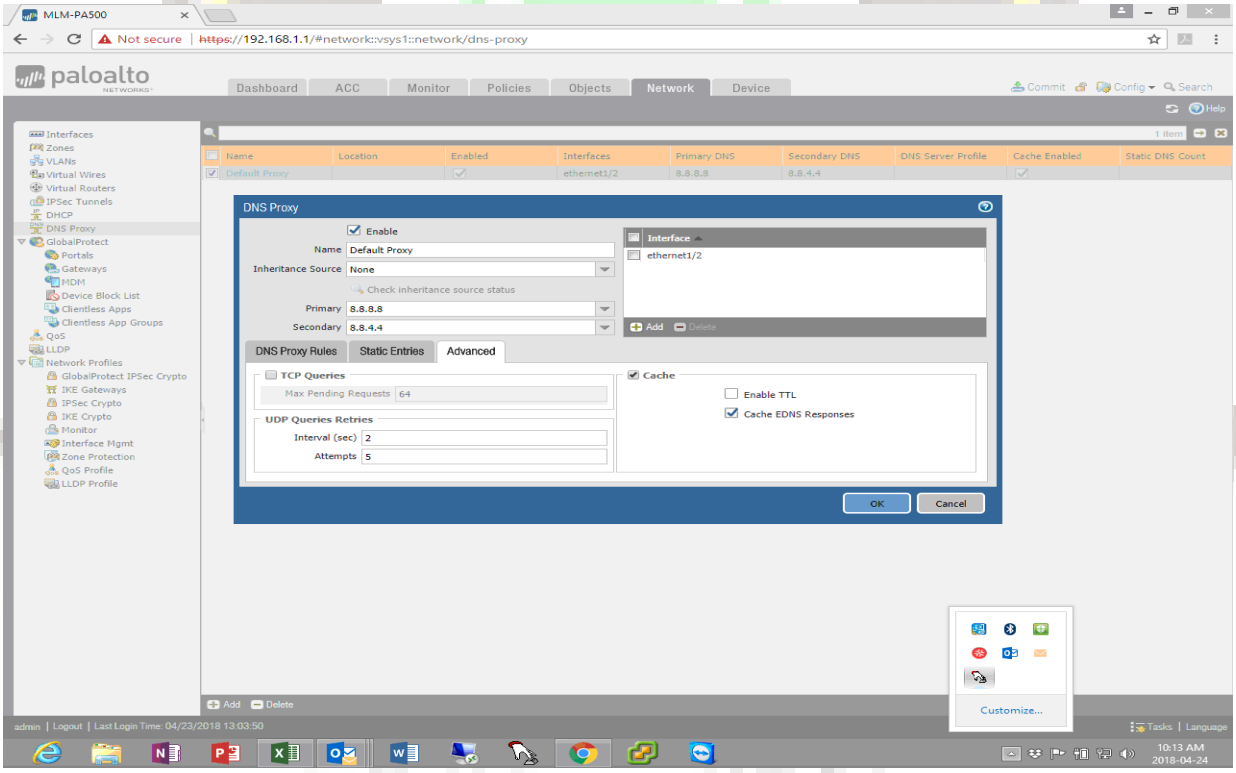
25. FIREWALL ACCESS MECHANISMS



All MLM firewalls must have unique passwords or other access control mechanisms. The same password or access control code must not be used on more than one firewall. Whenever supported by the involved firewall vendor, those who administer MLM firewalls must have their identity validated through extended user authentication mechanisms. In certain high security environments designated by the ICT Manager, such as the MLM Internet commerce site, remote access for firewall administrators is prohibited. All firewall administration activities must take place in person and on site.

Current Default Proxy listed below.

8.8.8.8 and 8.8.4.4



Main Ethernet Lines Layer 3 Interphase, IPV4 Static.

Ping: 41.162.162.162/29

Ping: 41.162.162.164

Allow MGT: 192.168.1.254/24

26. STANDARD PRODUCTS

Unless advance written approval is obtained from the IT Management team, only those firewalls appearing on the list of approved vendors and products may be deployed with MLM networks. All firewall interfaces and features deployed, such as virus screening, must be consistent with the Information Architecture issued by the ICT department.

27. APPROVALS

MATJHABENG LOCAL MUNICIPALITY

DOCUMENT CONTROL

DOCUMENT DETAILS

Author	PLM Rakotsoane
Company Name	Matjhabeng Local Municipality
Division Name	Information & Communication Technology
Document Name	Laptop Policy & Guidance
Version Date	05/03/2019
Effective Date	
Review Date	

Stakeholder Sign–off

Name	**Position**	**Signature**	**Date**
PLM RAKOTSOANE	ICT Manager		
TUMELO MAKOFANE	Executive Director SSS		
THABISO TSOAELI	Municipal Manager		

Security Sign-off

Name	Position	Signature	Date
PLM RAKOTSOANE	Acting ICT Manager		

1. PURPOSE

The purpose of this policy is thus to provide fairness in the procurement and allocation of notebook or laptop personal computers for use by employees as a work facility, to protect the confidentiality, integrity and availability of Matjhabeng Municipality's information by controlling access to its laptops and to provide guidelines for the use of laptops.

2. SCOPE

The scope of this policy applies to:

- Any laptop owned by The Matjhabeng; and
- Any person authorised by The Matjhabeng to use the laptop.

3. POLICY

3.1. Policy Statement

The Matjhabeng's information system resources are assets important to The Matjhabeng's business and stakeholders and its dependency on these assets demands that appropriate levels of information security be instituted and maintained. At any given time, some of The Matjhabeng's information resources will be held on, or will be accessible from, laptops, of which a proportion will regularly be removed from The Matjhabeng's premises. It is The Matjhabeng's policy that appropriate access control measures are implemented to protect its information system resources, as held on or accessible from laptops, against accidental or malicious destruction, damage, modification or disclosure, and to maintain appropriate levels of confidentiality, integrity and availability of such information system resources.

3.2. Policy Objectives

The objectives of this policy with regard to the protection of information system resources as held on or accessible from laptops against unauthorised access are to:

- Minimize the threat of accidental, unauthorised or inappropriate access to electronic information owned by The Matjhabeng or temporarily entrusted to it;

- Minimize The Matjhabeng's network exposure, which may result in a compromise of network integrity, availability and confidentiality of information system resources;

- Minimize reputation exposure, which may result in loss, disclosure or corruption of sensitive information and breach of confidentiality; and

- Minimize the risk of physical loss of the laptop.

3.3. Policy Overview

The Matjhabeng information system resources, as held on or accessible from laptops, are important business assets that are vulnerable to access by unauthorised individuals or unauthorised remote electronic processes. Adequate precautions are required to prevent and detect unwanted access. Users should be made aware of the dangers of unauthorised access, and managers should, where appropriate, introduce special controls to detect or prevent such access.

3.4. Policy Maintenance

Supporting standards, guidelines and procedures will be issued on an on-going basis by The Matjhabeng ICT department. Users will be informed of any subsequent changes or updated versions of such standards, guidelines and procedures by way of e-mail or other relevant communication media. Users shall then have the obligation to obtain the current information systems policies from The Matjhabeng Intranet or other relevant communication media on an on-going basis and accept the terms and conditions contained therein.

4. POLICY REQUIREMENTS

The Matjhabeng's information system resources, as held on or accessible from laptops, shall be appropriately protected to prevent unauthorised access.

4.1. General

- Laptops are an essential business tool, but their very portability makes them particularly vulnerable to physical damage or theft. Furthermore, the fact that they are often used outside of The Matjhabeng's premises increases the threats from people who do not work for Matjhabeng Municipality and may not have its interests at heart.
- Laptops are especially vulnerable to physical damage or loss, and theft – either for resale or for the information they contain.
- If a laptop or any of its accessories is lost due to outright negligence, a staff member shall make good the loss financially. The current method of

recovering the lost to the equipment utilized by Procurement division will be used.

- The impacts of breaches of security involving laptops include not just the replacement value of the hardware but also the value of any data on them, or accessible through them. Information is a vital asset. The Matjhabeng depends very heavily on its computer systems to provide complete and accurate business information when and where required. The impacts of unauthorised access to or modification of, critical or sensitive data will usually far outweigh the cost of the equipment itself.

4.2. Access to on/off-line Information

The following guidelines must be observed.

- The physical security of any laptop being used by you is your personal responsibility, so you must take all reasonable precautions. Be sensible and stay alert to the risks.
- Keep your laptop within your possession and within sight whenever possible, especially in busy public places such as airports, railway stations or restaurants.
- Lock the laptop with a defcon cable while in the office; lock it away out of sight when you are not using it. Never leave a laptop visibly unattended in a vehicle. If necessary, lock it out of sight in the boot and ensure that your car doors are locked.
- A space has been reserved on a file server for a laptop user to periodically back/synchronize the data or documents on his or her PC. The onus to backup data and documents rests with the user.
- The data or documents on any personal computer are, in the first instance, the property of MLM. Archive regulations therefore apply to these data and documents.
- When you are engaged in a meeting and you leave your desk or table for coffee or tea break or lunch, log off from the operating system, and always ensure that your screen is locked every 10 minutes or so of keyboard inactivity, to prevent access to your data on your PC by other persons.
- An employee to whom a laptop has been allocated or provided is responsible for then safety and custodianship of the laptop in the office and outside the office. If

employee lost a laptop more than once, a replacement of that will be a PC, this is to protect Municipal information.

- Carry and store the laptop in a padded laptop bag or strong briefcase to reduce the chance of accidental damage.
- The ICT helpdesk maintain records of the make, model, serial number and The Matjhabeng's asset label of your laptop, then do not transfer it to the next person without ICT consent. If it is lost or stolen, you can contact them for this information. It is your responsibility to notify the Police immediately and inform the ICT helpdesk as soon as is reasonably practicable.
- Viruses are a major threat to the Organization and laptops are particularly vulnerable if their anti-virus software is not kept up-to-date. The anti-virus software will update automatically every time you connect to the Network. If you have reason to believe that this is not happening, please contact the ICT helpdesk for advice.
- Avoid opening any unexplained email attachments.
- Virus scans normally happen automatically but the ICT helpdesk can tell you how to initiate manual scans if you wish to be certain.
- Respond immediately to any virus warning message on your computer, or, if you suspect a virus (e.g. by unusual file activity,) please contact the ICT helpdesk at 3422. Refer to "Anti-Virus" section of Malicious Code Policy & Guidance for more information.
- Laptops must have correctly-configured firewall software installed and switched-on. If you have any reason to believe that this is not the case, please contact the ICT helpdesk at 3422.
- You are personally accountable for all network and systems accessed under your user ID, so keep your log in details secret.
- Laptops are provided for official use by authorised employees. Do not loan your laptop or allow it to be used by others such as family and friends.
- A laptop user shall not use the laptop for private financial gain.
- In particular, laptop control is defined as the means of ensuring that the variable subset of The Matjhabeng's electronic information resources which is held on or accessible from laptops is available only to persons authorised to view or process that information in accordance with pre-determined rules.

- Avoid leaving your laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine, also avoid leaving your laptop in the office when you knock off.
- The contents of a laptop screen are easily observed by someone sitting in close proximity. Please ensure that no sensitive or critical information can be viewed by an unauthorised person when using the laptop in a location away from The Matjhabeng's premises (e.g. a restaurant).
- Ensure that when you are connecting to The Matjhabeng network (LAN) that you do not have your wireless or 3G connections enabled as this could allow a bridging from external networks into our corporate network.
- Upon departure from service in the municipality, a laptop must be returned to the ICT Manager. It is the employee's responsibility to obtain an acknowledgement of receipt.
- Both the supervisor and an employee shall be held personally liable for any loss incurred by the Department for a notebook that has not been deposited with ICT upon departure, this failure will impact an employee final package. An employee can still purchase a laptop at fair market value. Fair market value is designated as 25% of the purchase amount if a laptop has already exceeded its lifespan of 3 years. A purchase is subject to Municipal's approval.
- ICT remain responsible for recommending the new technologies, giving the specifications and the model of the laptops should be procured. Any employee wishes to deviate will be liable for additional costs whereas the laptop will remain Municipal property.
- This Policy may be used with Laptops terms of Use.

4.4. Policies

Laptops are subject to The Matjhabeng's full range of policies. Please ensure that you are familiar with them.

A laptop being used in an external location is no different from the point of view of applicability of policies from a PC being used within The Matjhabeng's premises.

4.5. Backups

If file content is being changed and is not transferred regularly to the corporate network, it is your responsibility you must take your own backups of data on your laptop on a regular basis.

It is your responsibility to take regular off-line backups to a suitable storage (**U drive; OneDrive**). Backups must be encrypted and physically secured.

4.6. Health and Safety Aspects of Using Laptops

Laptops normally have smaller keyboards, displays and pointing devices than desktop systems.

Because these may be less comfortable to use, there may be an increased risk of repetitive strain injury. If you experience any symptoms whatsoever which might be caused by laptop use, please discontinue using it immediately and report the matter to the Health and Safety Department.

Do not balance the laptop on your knees as this can cause back injury. Wherever possible, place the laptop on a conventional desk or table and sit comfortably in an appropriate chair to use it.

4.7. Reporting Security Incidents

All security incidents, including actual or potential unauthorised access to the Matjhabeng's information systems via laptop, should be reported immediately to the ICT Manager.

4.8. User Awareness

Users shall be made aware of their responsibilities in the prevention of unauthorised access to Matjhabeng information resources via laptop, including, but not limited to:

- That no equipment is left logged-in without the protection of an activated password protected screensaver;
- The need to be aware of this Policy and all its provisions.

5. STAFF MEMBERS TO WHOM LAPTOPS MAY BE PROVIDED

- All below laptop applicants SHOULD be in possession of the vehicle. Proof of vehicle ownership should be attached on the application.
    - The Mayor of Matjhabeng Municipality.
    - The Speaker of Matjhabeng municipality.
    - The Chief Whip of Matjhabeng municipality.
    - Members of Mayoral Committee of Matjhabeng Municipality.
    - Section 57 Managers.
    - The Senior Managers of Matjhabeng Municipality.
    - Managers of Matjhabeng Municipality.
    - Personal Assistants
    - Work study officers
    - Project managers.
    - Internal Auditors
    - Technical support staff, for example, information Technology Officers/technicians.
    - Staff members whose duties include Departmental research or
    - Anyone who is a member of legislated Council Meeting.

6. INSURANCE

- Laptops are thus insured.
- Members of staff should take note that household insurance does not cover employer property located in the house of a staff member.
- Members of staff are either liable for payment of excess fee for the laptop replacement or replacement costs in case the insurance do not replace an item and it's proven that it's due to negligence.
- Conditions leading to insurance claims rejections:
    - Late claims submission;
    - Jam locking incidents
    - Non-Forcible entry (***Stolen without breaking doors, windows or walls)***

7. SOFTWARE LICENSING

Only software that has been licensed by the MLM may be loaded on a laptop.

8. SECURITY GATE PASS CONTROL

Laptops shall be checked out and checked in with security at entrance gates. Gate security shall record the make, model and departmental inventory numbers in a register

9. DISCIPLINARY PROCESS

The Matjhabeng reserves the right to audit compliance with the policy from time to time. Any disciplinary action, arising from breach of this policy, shall be taken in accordance with The Matjhabeng's Rules and Disciplinary Code as amended from time to time. Disciplinary action may ultimately lead to dismissal.

10. DEVIATIONS FROM POLICY

Unless specifically approved, any deviation from this policy is strictly prohibited. Any deviation to or non-compliance with this policy shall be reported to the ICT Manager.

11. CONCLUSION

- This policy is short, and this should enable staff members to commit to memory the stipulations contained herein. By making use of a laptop, a staff member implicitly acknowledges this policy and agrees to abide by the policy in its entirety.
- This policy is subject to change from time to time.

Information Communication and Technology (ICT)

USER AND SYSTEM ACCESS POLICY

Matjhabeng Local Municipality

(MLM)

Contents

1.INTRODUCTION

With evolving technology along with increased risks and threats results in ensuring that a comprehensive user and system access controls are in place to mitigate against threats that could severely jeopardize MLM business critical applications and services. Information security user access controls provides a sound platform that ensures that ICT systems, data and infrastructure are continuously protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as restrictions of unauthorized disclosure or incorrect processing of data.

2.OBJECTIVE AND PURPOSE OF THE POLICY

The objective of the policy is to define the user access management control measures for the MLM ICT systems, information and infrastructure where it would apply to both the MLM users and Service Providers. This policy seeks to protect the privacy, security and confidentiality of the MLM information. The main objective of this policy is to provide the MLM with best practice User Access Management controls and procedures to assist in securing the user access management procedure.

The aim of this policy is to ensure that the MLM conforms to standard user access management controls in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that risks associated to the management of user access are mitigated. Formal procedures must control how access to information is granted and how such access is changed. This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

3.SCOPE

The ICT User Access Management Policy has been developed to guide and assist MLM to be aligned recognised best practice User Access Management controls and procedures. The policy applies to everyone in the MLM, including its service providers/vendors. This policy is regarded as being crucial to the operation and security of ICT systems of the MLM. The policy covers the following elements of user access management:

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

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

4.DEFINITION

Access control rules and procedures are required to regulate who can access MLM Information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing MLM information in any format, and on any device.

5.ADMINISTRATION OF POLICY

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

6.DELEGATION OF RESPONSIBILITY

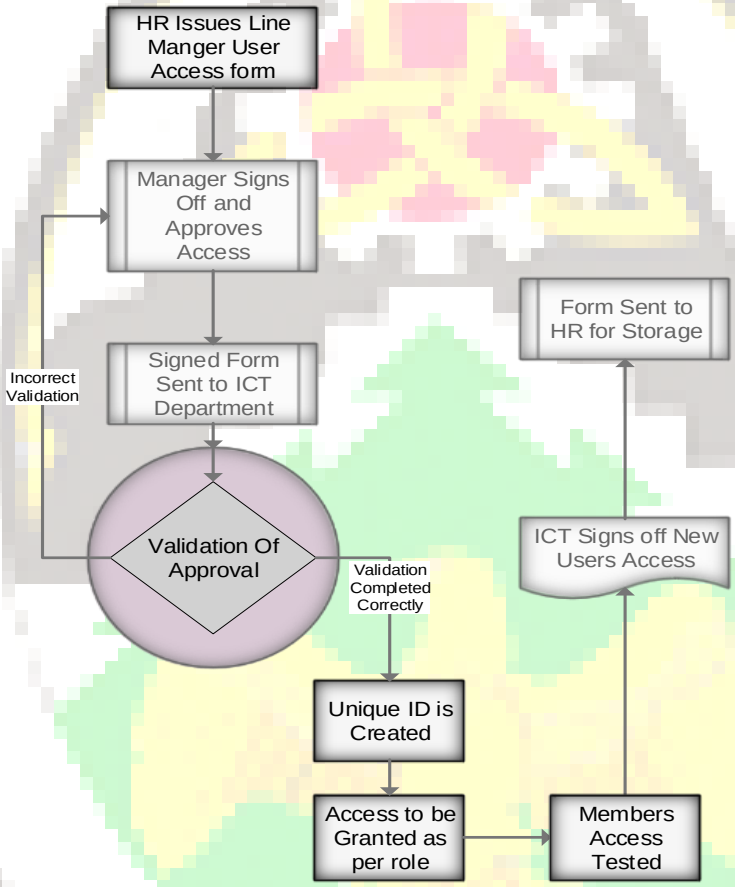
In accordance with the ICT Governance Policy, it is the responsibility of the Municipal Manager to determine the delegation of authority, personnel responsibilities and accountability to Management with regards to the Corporate Governance of ICT.

7.NEW USER REGISTRATION

A formalised user registration process must be implemented and followed in order to assign access rights. All user access requests must be formally documented, along with the access requirements, and approved by authorised personnel by making use of the user access request form. The template for this type of request can be found attached to this policy in Annexure A.

- User access requests must be obtained from HR on registration of a new employee.
- The form must be sent to the service provider/line manager for access requirements to be requested.
- Once the requirements have been requested and signed off by the departmental manager, the form must be sent to the ICT department for approval following which the activation of the employee based on the specified requirements will be completed.

- User access must only be granted once approval has been obtained.
- The form must then be sent back to HR for record keeping purposes. Records of user access granted must be stored for a minimum of 10 years.
- All users must be assigned unique user IDs in order to ensure accountability for actions performed. Should shared accounts be required to fulfil a business function, this account must be approved and documented by the Risk Management Committee.
- The diagram below depicts the formal new user registration process to be followed.



The unique ID must be associated with the HR and easy for members' recognition.
Examples:

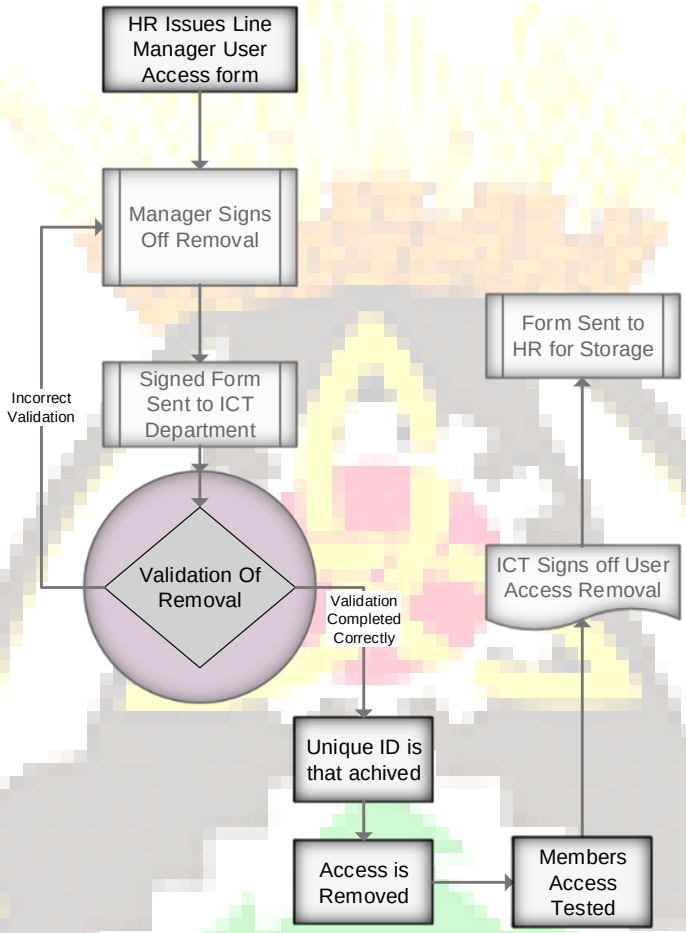
Name.Surname

Surname.Name

Surname.Name.EmployeeNum

8.TERMINATED USER REMOVAL

- A formalised user termination process must be implemented and followed in order to revoke access rights.
- All user termination requests must be formally documented and approved by duly authorised personnel. Access must be disabled immediately, with accounts being removed after 6 months once authorisation has been obtained by line manager.
- Terminated user requests must be obtained from HR on the termination of an employee. The template for this type of request can be found attached to this policy in Annexure A. The form must be sent to the service provider/line manager for access revocation to be signed off. Once access revocation has been signed off, the form must be sent to the ICT department for approval and deactivation of employee based on specified requirements. The form must then be sent back to HR for record keeping purposes. Records of user access removal must be stored for a minimum of 10 years.
- The diagram below depicts the formal user termination process to be followed:



9. USER PERMISSION/ROLE CHANGE REQUEST

- A formalised user access management process must be implemented and followed in order to adjust user access rights.
- All user access change requests must be formally documented, along with their access requirements, and approved by duly authorised personnel.
- Access must only be granted once approval has been obtained by the respective line manager.
- User access change requests must be obtained from HR on change of an employee's role or permissions. The template for this type of request can be found attached to this policy in Annexure A. The form must be sent to the service provider/line manager for access requirements to be signed off. Once the access requirements have been signed off, the form must then be sent to the ICT department for approval and adjustment of employee's access rights based on specified requirements. The form must then be sent back to HR for

record keeping purposes. Records of user access granted and removed must be stored for a minimum of 10 years.

- User access rights that are no longer required must be removed immediately.
- The diagram below depicts the formal user permission/role change request process to be followed. **WHERE IS A DIAGRAM?**

10. GENERAL USER ACCESS RIGHTS ASSIGNMENT

- Access rights include, but are not limited to:
- General office applications (E-mail, Microsoft Office, SharePoint, etc.);
- Department specific applications and/or databases;
- Network Shares;
- Administrative tasks;
- RAS/VPN Access (Remote Access Services and Virtual Private Network)
- Wi-Fi; and
- BYOD (Bring your own devices), this will be fully treated as other Municipality devices.
- Access must follow a “principle of least-privilege” approach, whereby all accesses revoked by default and users are only allowed access based on their specific requirements.
- The levels or degrees of access control to classified information must be restricted in terms of legislative prescripts.
- Access rights must be assigned to a group/role. User must then be assigned to that group. Access rights must not be assigned to individual users. **CLARIFY**

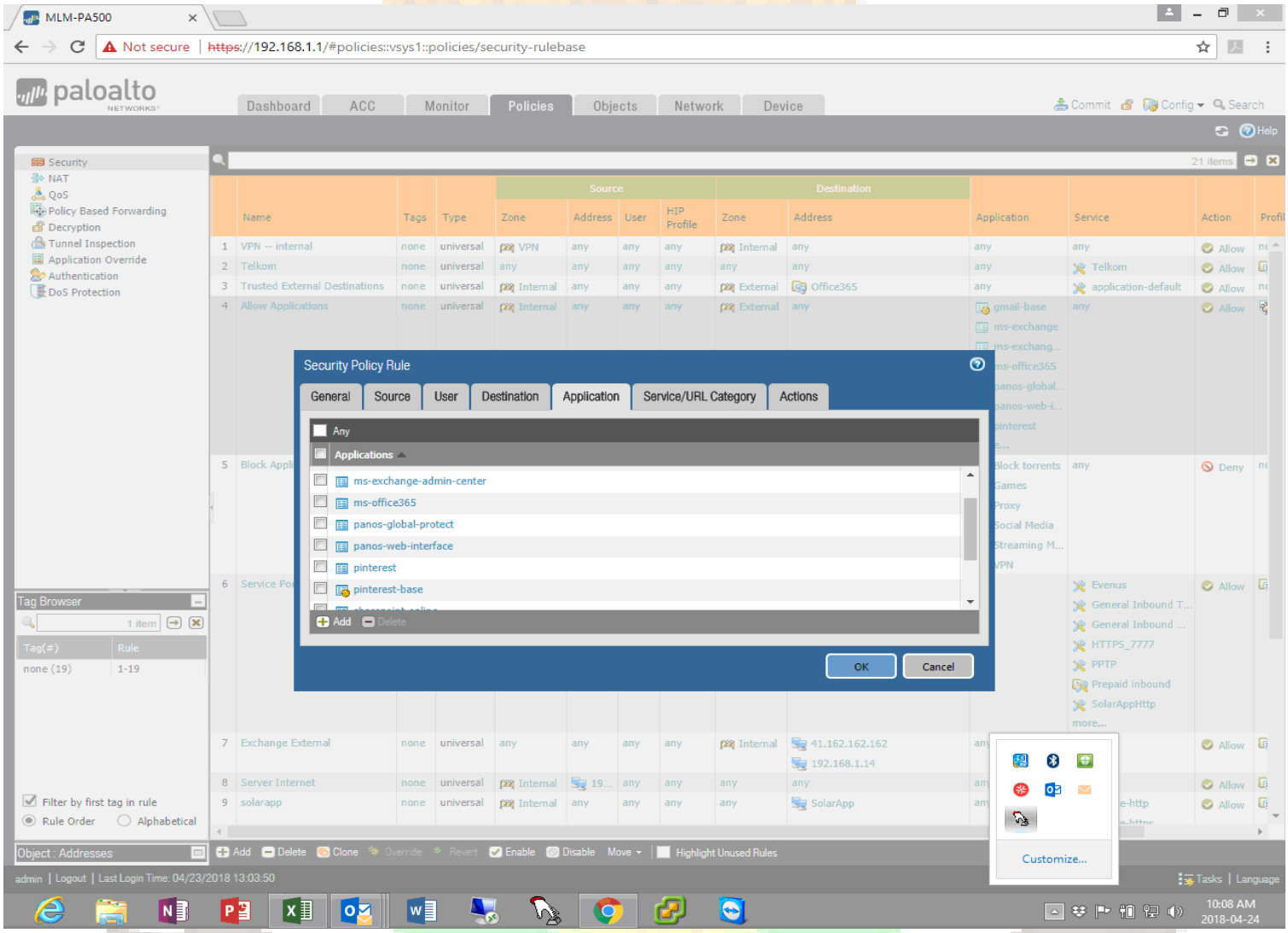
Restricted Access will fall on domains that have been block from accessing specific websites like for example:-

- Social Media Sites (What’s App, Facebook, Instagram etc.
- Streaming Video (Pinterest, You Tube, Supersport, on-line VOD sites)
- Porn
- All restricted sites – This will be based on the firewall SSL sites for intrusion.

Certain IP addresses will conform to the unrestricted usage of the internet but the integrity of the system must still be maintained.

The allowed list must be within the policy of MLM and must be maintained as key security infrastructure as per the policy rules and regulations current adjustment include the blocked list of websites.

The image below illustrates current list of allowed internet based content and/or sites:



11. NETWORK USER ACCESS RIGHTS ASSIGNMENT

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

- Access to Wi-Fi must only be provided to users who require access to the network throughout the Municipality, to fulfil their business function.
- RAS/VPN access must only be granted to users who require the service to fulfil their business function.
- Best practice states that RAS access must only be granted to employees who require remote access to a system in order to administer the environment.
- Best practice states that VPN access must only be granted to employees who:
  - Work remotely (Not at the office).
  - Work overtime, or not within regular office hours.

- It is the responsibility of the ICT Steering Committee to ensure all users must be made aware of the security risks and obligations associated with RAS/VPN access.
- RAS/VPN access must be monitored and audit logs reviewed every quarter (3months) by system administrators.
- All reviews must be formally documented and signed off by the ICT Manager.
- Documentation must be kept for record keeping purposes.
- RAS/VPN access reviews must be stored for a minimum of 10 years.
- The ICT Manager must approve all hardware and software, owned by Municipal employees and service providers/vendors, if it is used for official purposes (BYOD).
- The ICT team must ensure that all mobile devices are protected with a PIN.

12. PASSWORDS

Choosing passwords

Passwords are the first line of defence for our ICT systems and together with the user ID help to establish that people are who they claim to be. A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of our computers and systems.

Weak and strong passwords

A *weak password* is one which is easily discovered, the basic weak passwords are for example:

"Password123, GOD, Children's names, Spouse's-close relationship names"

A *strong password* is a password that are designed to be difficult to determine by the individuals that are not the owner of the set password:

Everyone must use strong passwords with a minimum standard of:

- At least seven characters.
- Contain a mix of alpha and numeric, with at least one digit
- More complex than a single word (such passwords are easier for hackers to crack).

Passwords should be alpha numeric and changed once a month as set by standard best practise. This can be managed and instituted on a server level.

Example: pinray45

Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different MLM systems.

Do not use the same password for systems inside and outside of work

Changing Passwords

All user-level passwords must be changed at a maximum of every 30 days as per the security policy of MLM, or whenever a system prompts you to change it. Default passwords must be changed immediately. If you are aware, or suspect, that your password has become known to someone else, you **must** change it immediately and report your concern to IT Helpdesk at MLM Users **must not** reuse the same password within 12 password changes

13. OPERATING SYSTEM ACCESS RIGHTS ASSIGNMENT

Each system administrator must be given their own accounts within the administrator group. Should the need arise for shared accounts being required to fulfil a business function, then this account must be approved and documented by the Risk Management Committee. The default guest account must be removed or renamed and disabled.

14. APPLICATION USER ACCESS RIGHTS ASSIGNMENT

Segregation of duties must be practiced, in such a way that application administrators cannot perform general user tasks on an application. This is to prevent any fraudulent activity from taking place. Applications administrators must remain independent of the department utilising the application, with the exception of the ICT department.

15. DATABASE USER ACCESS RIGHTS ASSIGNMENT

- The ICT Manager must limit full access to databases (e.g. sysadmin server role, db_owner database role, sa built-in login etc.) to ICT staff who need this access.
- Municipal employees who use applications may not have these rights to the application's databases.
- The ICT Manager must ensure that Municipal employees who access databases directly (e.g. through ODBC) only have read access.
- The ICT Steering Committee must approve all instances where Municipal employees have edit or execute access to databases.
- The ICT Manager must review database rights and permissions on a quarterly basis (every 3 months). Excessive rights and permissions must be removed.

16. REVIEWING USER ACCESS AND PERMISSIONS

- User access and user permissions must be reviewed every quarter (3 months) by system administrators.
- On a monthly basis, HR must send a list of all terminated employees for that month to the ICT department. This list must be used to ensure that all terminated users have had their access revoked. Should one or more terminated users still have access to the environment, an investigation into the finding must be conducted.

- On a monthly basis, the ICT Manager must review all users with administrative access to the environment and assess their rights for appropriateness. Should a user be found with excessive rights, a user access change request must be performed.
- All reviews must be formally documented and signed off by the ICT Manager.
- Documentation must be kept for record keeping purposes. Records of user access review must be stored for a minimum of 10 years.

17. USER RESPONSIBILITIES

It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to MLM systems by:

- Following the Password Policy Statements outlined above in Section 6.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing IT Helpdesk or the ICT manager of any changes to their role and access requirements. Please note attached Annexure A – User Access Change Document

18. USER AND ADMINISTRATOR ACTIVITY MONITORING

- User and administrator activity must be monitored through audit and event logging.
- Once a month, system administrators and application owners must review audit and event logs for suspicious and malicious activities.
- Dormant accounts should be disabled and a request to remove the access should be performed in line with policy. User Permission/Role Change Request.
- All reviews must be formally documented and signed off by the ICT Manager.
- Documentation must be kept for record keeping purposes. Records of user activity monitoring must be stored for a minimum of 10 years.

ANNEXURE A: USER ACCESS MANAGEMENT FORM EXAMPLE

Name: _____ Date: ___/____/____

Designation: _____Requested by: _____

Department:_____

Please Tick What is Required	
PC ☐ *Laptop☐	
Administrative rights	
E-mail	
VPN	
RAS	
Solar – List all required function in **Appendix A**	
Payday HR ☐ Payday Salaries☐	
Cashdrawer	
Own Device setup	
Other: Specify	

New Application	
Change Of Details/Additional Access	
Removal of Access	

_____

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

Period of access: _____

Reason for request:

_____

_____

HR Manager Line Manager ICT Manager System Administrator

Signature: _____ _____ _____ _____

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

***ATTACH PROOF OF CAR OWNERSHIP**

TERMS AND DEFINITIONS

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

MATJHABENG

MUNICIPALITY

1. POLICY STATEMENT

i. This policy is established as guidance to employees, who by the nature of their work, are required to be accessible by telephone/e-communication regardless of the time of day, day of the week, or geographical location. Municipal Manager and Department heads will determine service equipment and the type of services necessary to fulfil specific Municipality responsibilities although a Municipal Manager has a final say on who gets the contract voice (***cell phone***) and data (***3G, WiFi, Tablet, etc***) and why. Costs related to these services will be the responsibility of the Municipality.

ii. Municipality employees are strongly discouraged from using a Municipality provided wireless devices for personal business or conducting Municipality business on any wireless devices while operating a motor vehicle. Employees are encouraged to use "hands-free" phones in limited situations and not for prolonged conversation. Wireless devices use while driving should only occur in an emergency situation.

iii. This policy applies to all wireless devices contracts entered into by Matjhabeng Municipality employees, effective as of the date of this policy. Department heads may establish wireless devices use policies that are more but not less restrictive than this policy.

2. PURPOSE

(i) This policy establishes guidelines for procurement, possession, and appropriate use of Municipality-owned wireless devices.

(ii) To define guidelines for the reimbursement of personal calls and services by the employee to the Municipality

(iii) To provide guidelines on the acquisition and use of wireless devices for councilors and other officials.

(iv) To reduce unnecessary wireless device costs to the Municipality and to avoid violation of state mandates regarding cellular phone/3G card/WiFi/Tablet use.

3. ENTITIES AFFECTED BY THE POLICY

All Matjhabeng Municipality full and part-time employees, including wage employees. This policy also governs wireless devices acquired via grants and contracts awarded in Matjhabeng Municipality's name.

4. CRETERIA FOR ALLOCATION OF WIRELESS DEVICES REIMBURSEMENTS.

(i) Cognizance should be taken of the fact that there are strategic posts within the council and there are members of council whose responsibilities are of such a nature that they need wireless devices.

(ii) Only Executive Mayor, The Speaker, Chief Whip, all full time councilors, Municipal Manager and Executive Directors qualify for wireless devices reimbursements.

(iii) It is imperative that sufficient funds are available in the budget for these expenses.

5. GENERAL CONDITIONS

(i) Wireless devices must be obtained by means of rental agreement by each individual member of council.

(ii) The contract entered into by each individual member of council forms the basis for reimbursements.

(iii) The reimbursements should not be seen as an allowance, because it will then be taxable.

(iv) Council is responsible for rentals and subscriptions for officials, if the handsets/devices chosen by the councilor/official exceed what package offers, councillor/official will be liable to pay the excess amount.

6. AUTHORITY TO APPROVE

6.1 CONCILLORS, CHIEF WHIP, SPEAKER AND ANY POLITICAL OFFICER'S REIMBURSEMENT

(i) The Executive Mayor or his delegate (***Chief of Staff***) has the authority to approve or reject applications (motivation letter/submission) for wireless devices based on this policy. Manager ICT/cell or wireless device Administrator will also have an authority to recommend or do not recommend based on whether the applicant do or don't qualify in terms of the policy. If the applicant is dissatisfied, he/she may escalate matter to either Executive Mayor or his delegate (chief of staff) depending on who has rejected the application.

(ii) An application form must be completed, and the councilor must inform the Cellphone Administrator if a contract for the wireless device is cancelled.

(iii) Determined by the **CIRCULAR 04/14 DETERMINATION OF UPPER LIMITS OF SALARIES, ALLOWANCES AND BENEFITS OF COUNCILLORS FOR 2013/14 FINANCIAL YEAR.**

(iv) Final approval will be done by the Municipal Manager.

6.2 OFFICERS' REIMBURSEMENT

(i) The Supervisor, the relevant Executive Director or/and will have the authority to either recommend or not recommend applications (motivation letter/submission) for wireless devices. Manager ICT/cell or wireless device Administrator will also have an authority to recommend or do not recommend based on whether the applicant do or don't qualify in terms of the policy. If the applicant is dissatisfied, he/she may escalate the matter to either his/her HOD or the Municipal Manager depending on who has rejected the application.

(ii) An application form must be completed, and the individual official must inform the Cellphone Administrator if a contract for the wireless device is cancelled.

7. LOSS OR THEFT OF OR DAMAGE TO WIRELESS DEVICES (*cellphone and tablets ONLY*)

All devices are insured and users ***ALL*** liable to pay excess amount in case the claim is approved. If however any damage or loss occurs as a result of negligence on the part of wireless devices holder, and the insurance doesn't pay, the repair and procurement costs to such damages shall be borne by the said official or councilor.

8. INTERNATIONAL ROAMING

International roaming **should** be deactivated by default, international shall not by any means be activated on any device/account for any reason/purpose.

The user will be liable for all the costs resulted from international calls.

9. INSURANCE

The Municipality has covered ALL the devices in case of the theft, loss and damage.

10. PROCEDURE

(i) SERVICE INTERNAL APPLICATION

- The detailed motivation letter that explains why an applicant should have the service must be written and be recommended by the supervisor/manager and a relevant director of the applicant, funds be confirmed by Finance department, recommendation based on whether the applicant do or don't qualify for the service by ICT Manager/Wireless device Administrator. The CFO will either recommend or not, and then the final approval be made by the Municipal Manager.
- Signed applicant motivation letter will be processed by ICT and application forms from Service Provider be filled and send to both the CFO and the Municipal Manager for the signatures. The accompanying letter to the Service Provider signed by the Municipal Manager together with the Application form will be sent to the Service provider.

(ii) ACQUISITION

- The council shall enter into contract with a wireless devices service provider for the acquisition and use of wireless devices on behalf of councilors and qualifying officials or individual may enter into contract after the approval of Mayor in the case of councilors or the Municipal Managers in the case of officials.

- Wireless devices will either remain the property/ies of the Municipality after the contract of 24 months has expired, or the user pay 20% of the device's initial amount/value.

(iii) TERMINATION OF SERVICE

- Should an employee/councillor leave the municipality s/he will have to return the wireless device and sim card on or before his/her last day of employment within the Municipality.

- Should an employee/councillor be suspended s/he will have to return the wireless device together with a sim card on or before his/her last day of employment with the municipality and it will be kept until s/he returns.
- Should an employee/councillor stops acting in a supervisory capacity s/he will have to return the wireless device and sim card on or before his/her last day of her/his acting position.
- The transfer of the wireless device or the wireless device to the employee will be possible under the following circumstance;
    - Her/his work contract with the Municipality expires and wish to continue using the number, in this case s/he must write the letter to request the Municipal Manager's approval of contract transfer to her/his names and s/he will be liable for ALL contract's costs.
    - S/he leaves the Municipality with whatsoever reason but wish to continue using the number, in this case s/he must write the letter to request the Municipal Manager's approval of contract transfer to her/his names and s/he will be liable for ALL contract's costs and
    - S/he paid finance deal for the device s/he has chosen, in this case s/he must write a letter to the salaries department to give a consent of a monthly salary deduction for the period of two years or once off. This will be determined by the difference between the subsidy amount and a line debited amount.
- Else **ALL** the devices remain Municipality's property.
- If however s/he wish to keep a device after a period of 2 years, an official may do so under one condition;

- S/he pays a certain percentage that will be determined by period the devices has been used multiply by original price. **NB: *See table below*.**

Months used	Percentage of original price
0-3	100%
3-6	75%
6-12	60%
12-18	45%
18-24	20%

(iv) MONTHLY ACCOUNTS/LIMITS

- It is the responsibility of the users to check their balances. In case the limits are exceeded, the account statements will be sent to Salaries Division, and the deductions of an excess amount will be done from salaries accordingly.

QUALIFYING OFFICIALS AND ALLOCATION OF FUNDS

OFFICIALS	VOICE	PACKAGE	DATA	PACKAGE
The Mayor	Determined by Circular-04-Jan-2014-Determination-of-Upper-Limits-of-Salaries		R269	MyGig5
The Speaker	Determined by Circular-04-Jan-2014-Determination-of-Upper-Limits-of-Salaries		R269	MyGig5
The Chief Whip	Determined by Circular-04-Jan-2014-Determination-of-Upper-Limits-of-Salaries	Red Executive	R269	MyGig5
MMCs	Determine by Circular-04-Jan-2014-Determination-of-Upper-Limits-of-Salaries	Red Executive	R269	MyGig5
Chief of Staff	R 2 099-00	Red Executive	R269	MyGig5
Senior Managers	R 769-00	uChoose Smart XL	R269	MyGig5
*# Acting Personnel	Will be determined by the position acting on		R269	MyGig5

OFFICIALS	VOICE	PACKAGE	DATA	PACKAGE
Municipal Manager	R 2 099-00	Red Executive	R269	MyGig5
Executive Directors	R 2 099-00	Red Executive	R269	MyGig5

Senior Managers	R 769-00	uChoose Smart XL	R269	MyGig5
*#Acting Personnel	Will be determined by the position acting on		R269	MyGig5

11. OTHER EMPLOYEES AND FUNDS ALLOCATION

Any employee whose job requires that s/he be able to be contacted urgently and / or for whom possession of wireless devices are essential requirements for the performance of his / her job, may apply for a cell phone SIM only plan.

POSITION	Price plan	Cost with SIM only	Monthly minutes (Double)	Monthly Megs (Double)	Free SMSs
*Other employees	uChoose Smart S	R229	75*2 = 150 minutes	200*2 = 400 MB Data	400 SMSs
*Managers	uChoose Smart L	R579	250*2 = 500 minutes	500*2 = 1 GB Data	1000 SMSs
*Communication, Marketing & Branding Officer	uChoose Smart XL	R809	400*2 = 800 Minutes	800*2 = 1.6 GB Data	1600 SMSs
*# Acting Personnel	Will be determined by the position to act on.				

* Motivation letter is required, neither recommendation nor approval is guaranteed, (clause i and ii of 6.1 and 6.2).

It is a responsibility of the acting personnel to inform the Municipal Manager and ICT if stops acting on a supervisory capacity, therefore hand back the municipal's device/s.

1. WHO SHOULD READ THIS POLICY?

· Executive Mayor, Chief Whip, Speaker and Members of Mayoral Committees

· Municipal Manager, Executive Directors, Senior Managers and Managers

· Employees requiring wireless device access

· Individuals acting in a supervisory capacity

· Procurement Personnel (Wireless device administrator)

· Accounts Payable – Salaries section

· ICT Manager