MATJHABENG CORPORATE GOVERNANCE FOR INFORMATION, COMMUNICATION AND TECHNOLOGY POLICY

(MCGICTP)

Contents

Document Information

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

Distribution List

Name	Date	Phone/Fax/Email

Document Version History

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

1. INTRODUCTION

1.1 Matjhabeng's ICT

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

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

1.2 Definitions

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

This framework is viewed as encompassing the following strands:

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

1.3 Scope and Applicability

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

2. Adopted Frameworks

By adopting this framework, the following outcomes are anticipated:

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

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

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

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

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

2.2 ISO/IEC 38500

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

2.3 COBIT 5®

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

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

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

2.4 ITIL V3

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

3. MUNICIPAL PLANNING CONSIDERATIONS

3.1 Municipal Strategic Planning

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

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

3.2 ICT Strategic Plan

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

3.3 ICT Operations Plan

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

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

4. ENSURING MUNICIPAL ALIGNMENT

4.1 What is organisational alignment

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

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

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

4.2 Organisational Structure

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

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

4.3 ICT Governance Committee

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

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

Benefits of having an IT Steering committee include:

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

4.4 Best practice in governance steering committee

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

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

5. COMMITTEE SUMMARY

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

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

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

6. ACCOUNTABILITY & LEGAL MANDATE

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

6.1 Legislation

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

- Local Government Municipal Systems Act, Act 32, of 2000,
- Local Government: Municipal Structures Act, Act 117 of 1998,
- the Public Administration Management Act, Act 11 of 2014 and
- the Local Government: Municipal Finance Management Act, Act 56 of 2003.

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

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

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

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

6.2 Delegations

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

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

6.3 Financial Accountability

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

6.4 Information Management

6.4.1 Access to information

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

6.4.2 Information privacy

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

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

6.4.3 Corporate reporting

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

6.4.4 Corporate governance in the municipality

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

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

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

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

  And is in particular concerned with:

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

6.5 Governance of ICT in the municipality

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

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

Effective governance of ICT is implemented in Matjhabeng by:

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

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

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

Means and mechanisms;

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

Decision making mechanisms:

- Roles and responsibilities;
- Processes;
- Practices.

7. ICT DELIVERY

7.1 Principles for ICT governance

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

7.2 Table of ICT governance principles:

ICT GOVERNANCE PRINCIPLES
<u>Principle 1:</u> Political Mandate -The Governance of ICT must enable the municipality's political mandate:

- The Municipal Council must ensure that Corporate Governance of ICT achieves the service delivery mandate of the municipality.

Principle 2: Strategic Mandate - The Governance of ICT must enable the municipality's strategic mandate.

- The Municipal Manager must ensure that Corporate Governance of ICT serves as an enabler to the municipality's strategic plans.

Principle 3: Corporate Governance of ICT - The Municipal Manager is responsible for the Corporate Governance of ICT.

- The Municipal Manager must create an enabling environment in respect of the Corporate Governance of ICT within the applicable legislative and regulatory landscape and information security context.

Principle 4: ICT Strategic Alignment - ICT service delivery must be aligned with the strategic goals of the municipality

- Management must ensure that ICT service delivery is aligned with the municipal strategic goals and that the administration accounts for current and future capabilities of ICT. ICT must ensure that ICT is fit for purpose at the correct service levels and quality for both current and future Municipal needs are met.

Principle 5: Significant ICT Expenditure - Management must monitor and evaluate significant ICT expenditure.

- Management must monitor and evaluate major ICT expenditure, ensure that ICT expenditure is made for valid Municipal enabling reasons and monitor and manage the benefits, opportunities, costs and risks resulting from this expenditure, while ensuring that information assets are adequately managed.

Principle 6: Risk Management and Assurance - Management must ensure that ICT risks are managed and that the ICT function is audited.

- Management must ensure that ICT risks are managed within the municipal risk management practice. ICT must also ensure that the ICT function is audited as part of the municipal audit plan.

Principle 7: Organisational Behaviour - Management must ensure that ICT service delivery is sensitive to organisational behaviour/culture.

- Management must ensure that the use of ICT demonstrates the understanding of and respect for organisational behaviour/culture.

7.3 ICT governance oversight structure in the municipality

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

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

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

7.4 Roadmap towards municipal governance

Initial Considerations

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

Building sustainability entails:

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

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

7.5 Critical success factors for business / ICT relationship

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

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

7.6 Organisational structure

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

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

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

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

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

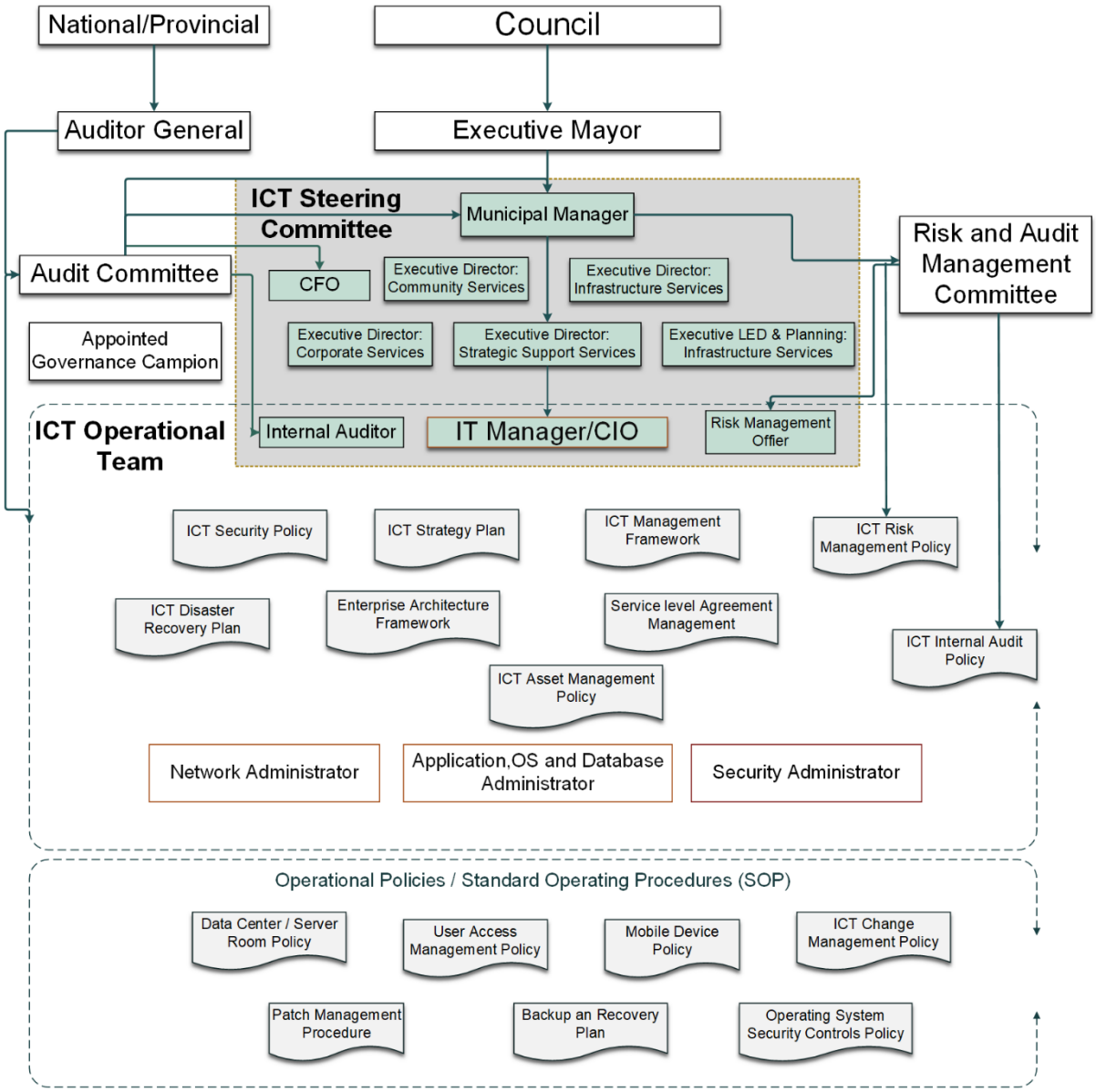


Figure 1 MCGICTP Organisational Structure

7.7 Municipal IT Steering Committee

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

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

7.8 ICT Manager / Chief Information Officer

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

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

7.9 Implementation

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

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

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

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

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

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

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

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

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

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

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

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

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

8. SHORT-TERM AND MEDIUM TO LONG TERM APPROACHES

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

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

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

Figure 2 RACI Mapping Model for Implementation

8.1 Short-Term

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

8.1.1 Security management

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

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

8.1.1.3 Carry out ICT security awareness initiatives.

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

8.1.1.5 Implement strong password controls to authenticate system access.

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

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

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

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

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

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

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

8.1.2 User access control

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

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

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

8.1.2.4 Independently monitor activities of system administrators.

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

8.1.3 Change management

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

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

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

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

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

8.1.4 Data center management

8.1.4.1 Control changes to database management software

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

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

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

8.1.5 Facilities and environmental controls

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

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

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

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

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

8.1.6.3 Implement an ICT backup and retention strategy.

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

8.1.6.5 Store backups in a secure offsite storage facility.

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

8.1.7 ICT Infrastructure

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

8.1.7.2 Assess the warranty status of all machines

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

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

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

8.2 Medium to Long term

The following initiatives will be considered and performed:

8.2.1 Develop an ICT strategic Plan that supports business requirement

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

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

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

8.2.5 Review ICT services performances periodically against targets.

8.2.6 Conduct regular ICT risk assessments to identify emerging risks.

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

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

8.3 ICT Governance Measurement

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

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

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

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

8.4 Support for governance

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

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

8.5 Recommendations towards sound ICT governance

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9. RISK MANAGEMENT

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

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

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

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

10. MAINTAINING THE ICT GOVERNANCE FRAMEWORK

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

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

11. TERMS AND DEFINITIONS

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

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

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

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

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

12. APPROVAL

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

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

Information Communication and Technology (ICT) Security Policy

Matjhabeng Local Municipality

(MLM)

Table of Contents

Document Information

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

Distribution List

Name	Date	Phone/Fax/Email

Document Version History

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

1. INTRODUCTION

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

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

2. SCOPE AND OBJECTIVES

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

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

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

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

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

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

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

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

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

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

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

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

3. APPICABILITY

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

4. RESPONSIBILITIES

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

5. POLICY DESCRIPTION

5.1 GENERAL

5.1.1 All employees using the Facilities are required to:

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

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

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

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

5.1.2 No User of the Facilities may:

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

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

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

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

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

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

5.1.4.3 Always subject to this Policy.

5.1.5 The Facilities may not be used for:

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

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

5.1.5.3 Unauthorised not-for-profit activities;

5.1.5.4 Private advertising of products or services;

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

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

5.2 IDENTITY AND ACCESS

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

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

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

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

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

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

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

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

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

5.2.9 If account is not used for more than 6 months, it will be disabled user verifies it.

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

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

5.3 THIRD PARTY AND REMOTE ACCESS

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

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

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

5.4 SECURITY

5.4.1 No User is allowed to use or work on in any way, a computer other than the computer allocated to that specific user by ICT, hence no private computers may be connected to the network, if that need arise, all administrators' passwords should be removed and use Municipality's passwords only.

5.4.2 All Users must safeguard their user-id and/or passwords and these are not to be shared with any other person without authorisation. Should a User become aware that their

password has been revealed to a third party, the User must immediately contact the ICT Security Administrator/helpdesk in order to disable the account and/or change the password. All Users shall report any attempted unauthorised use of their password of which they become aware.

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

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

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

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

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

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

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

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

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

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

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

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

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

business;

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

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

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

5.5 INFORMATION HANDLING

5.5.1 Unauthorised disclosure of sensitive information is prohibited.

5.5.2 Unauthorised tampering or alteration of sensitive information is prohibited.

5.5.3 Unauthorised destruction or disposal of sensitive information is prohibited.

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

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

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

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

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

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

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

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

5.6 CONFIDENTIALITY

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

5.6.2 The Facilities have no capability to enable the sending or receiving of private or personal, confidential electronic communications. The ICT Security Administrator has access to all

electronic mail and User access requests and will monitor messages as necessary to ensure efficient performance and appropriate use. Messages relating to, or in support of, illegal or unauthorised activities will be reported to the appropriate authorities.

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

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

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

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

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

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

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

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

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

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

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

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

5.7 INTERNET USAGE

5.7.1 No User shall:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.8 ELECTRONIC MAIL (E-MAIL)

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

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

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

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

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

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

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

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

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

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

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

6. ASSESSMENT AND COMPLIANCE

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

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

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

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

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

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

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

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

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

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

6.2.3 Radius and/or Tacacs audit trail logs

6.2.4 Applications and 3rd Party service provider access logs.

6.2.5 ICT Reporting and Management systems.

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

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

7. TERMS AND ABBREVIATIONS

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

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

8. APPROVALS

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

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

Information Communication and Technology (ICT) Strategic Plan

Matjhabeng Local Municipality

Table of Contents

Document Information

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

Distribution List

Name	Date	Phone/Fax/Email

Document Version History

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

1. INTRODUCTION

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

2. APPROACH

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

These drivers were considered as follows:

2.1 INPUTS FROM THE IDP

Back to Basic

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

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

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

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

- Putting people first
- Delivering basic services

- Good Governance
- Sound financial management
- Building Capacity

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

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

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

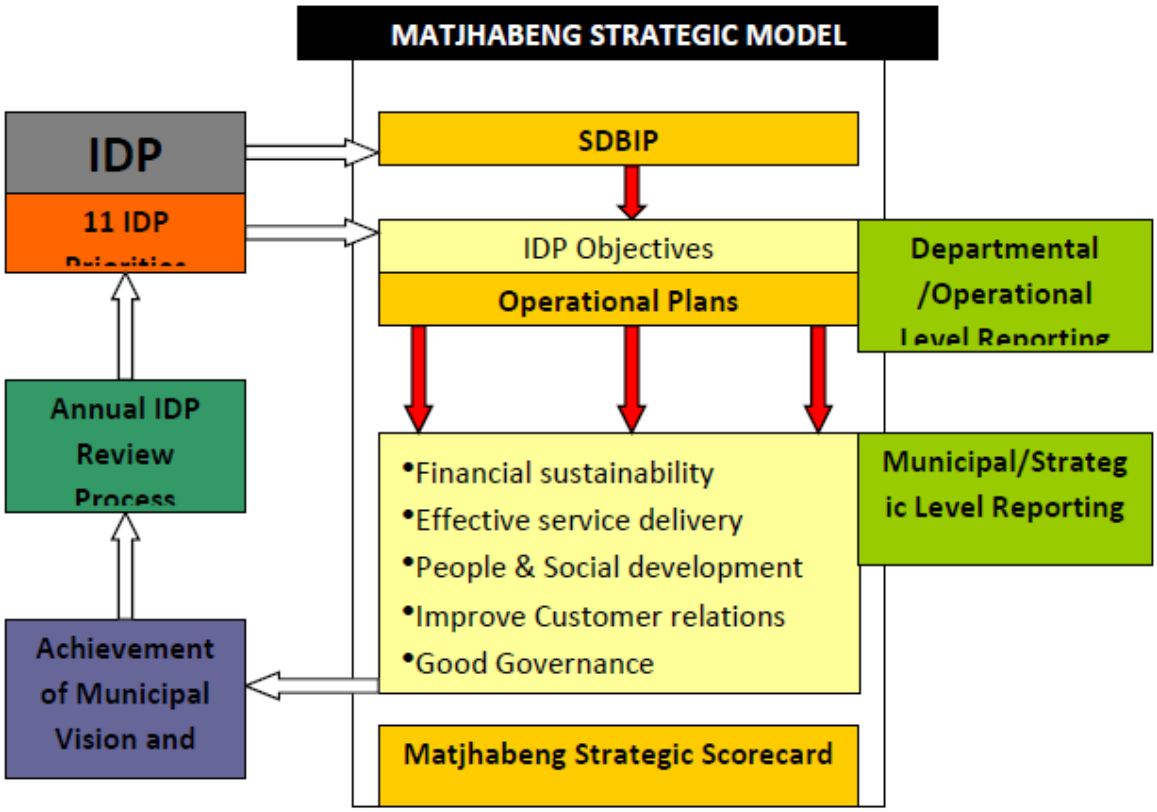


Figure 1: Matjhabeng strategic model from IDP

2.2 HOLISTIC APPROACH FOR INCLUSIVE ICT STRATEGIC PLANNING

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

This is succinctly represented as follows:

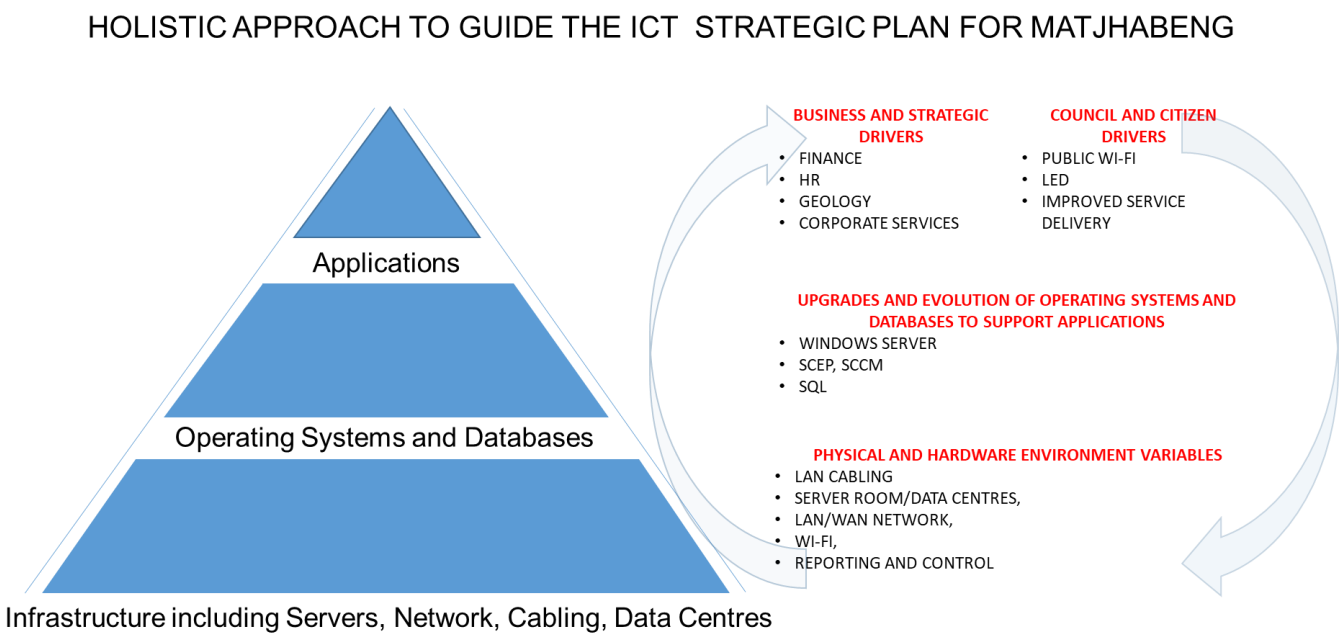


Figure 2: Strategic plan drivers

3. AS-IS ASSESSMENT SUMMARY

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

3.1 ICT ORGANIZATIONAL STRUCTURE

3.2 Head Office in Welkom

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

3.2.2 Overview of users and infrastructure supported by ICT:

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

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

3.3 Regional Sites/Units

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

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

TABLE 2: ICT Users and Infrastructure Overview – Regional Sites

3.4 Satellite offices listed below:

List of Satellite Sites:

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

TABLE 3: ICT Users and Infrastructure Overview – Satellite Sites

3.5 Network Connectivity diagram:

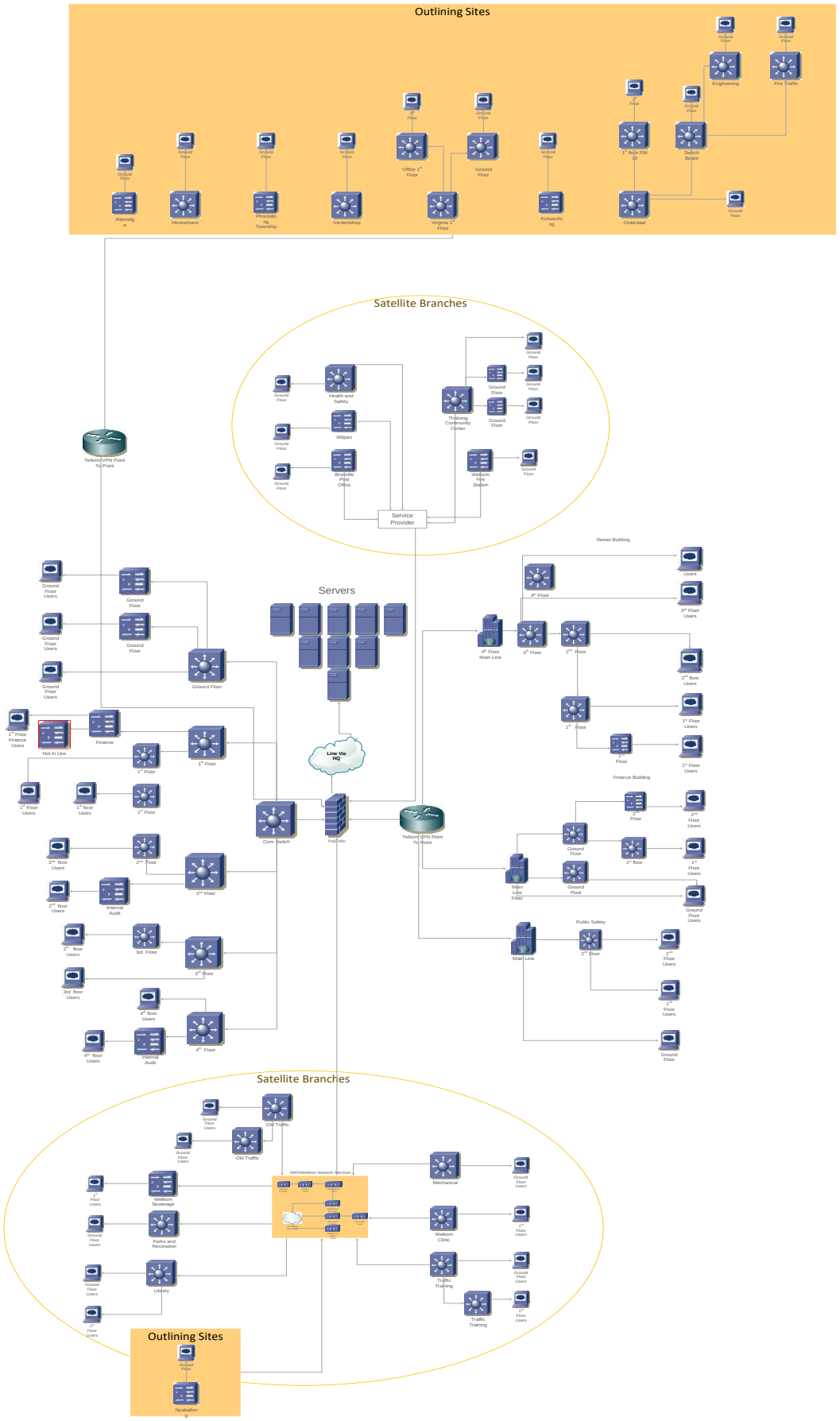


Figure 3: LAN/WAN Network Consolidated

3.6 Summary of Key applications used by the Business Units

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

TABLE 4: Key Applications Mapping for Business Units

3.7 ORGANIZATION STRUCTURE

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

implementation and headcount allocations that is tabled is reflected below:

Figure 4: ICT Organizational Structure

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

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

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

TABLE 5: SWOT ANALYSIS

5. GAP ANALYSIS SUMMARY

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

The current gaps are summarized below:

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

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

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

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

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

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

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

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

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

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

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

6. ICT IMPLEMENTATION PLAN

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

6.1 SHORT TERM

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

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

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

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

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

6.1.6 Revamp and readiness of Disaster Recovery Site in Virginia.

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

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

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

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

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

6.1.12 ICT Resourcing, training and development.

6.1.13 E-filing of all municipal documents.

6.2 LONG TERM

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

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

6.2.3 Intra-City broadband planning and implementation.

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

6.2.5 Cloud Implementation Strategy.

6.2.6 Digital Security assessment and implementation.

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

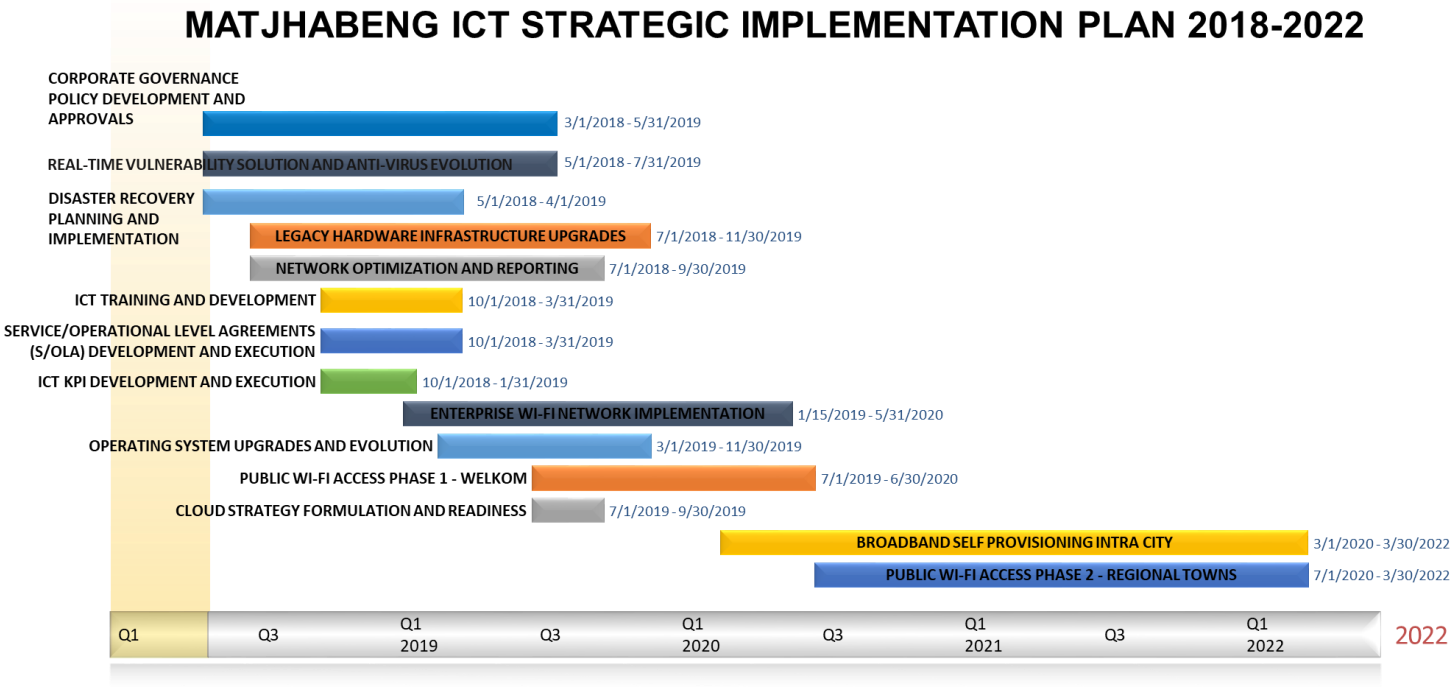


Figure 5: ICT Strategic Plan Implementation 2018-2022

7. APPROVALS

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

Table of Contents

Document Information

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

Distribution List

Name	Date	Phone/Fax/Email

Document Version History

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

Introduction

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

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

Scope

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

Policy description

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

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

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

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

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

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

Rules for Virus Prevention

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

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

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

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

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

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

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

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

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

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

ICT Responsibilities

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

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

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

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

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

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

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

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

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

Department and Individual Responsibilities

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

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

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

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

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

Policy enforcement

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

Declaration of understanding

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

Approvals

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

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

Information Communication and Technology (ICT) 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.

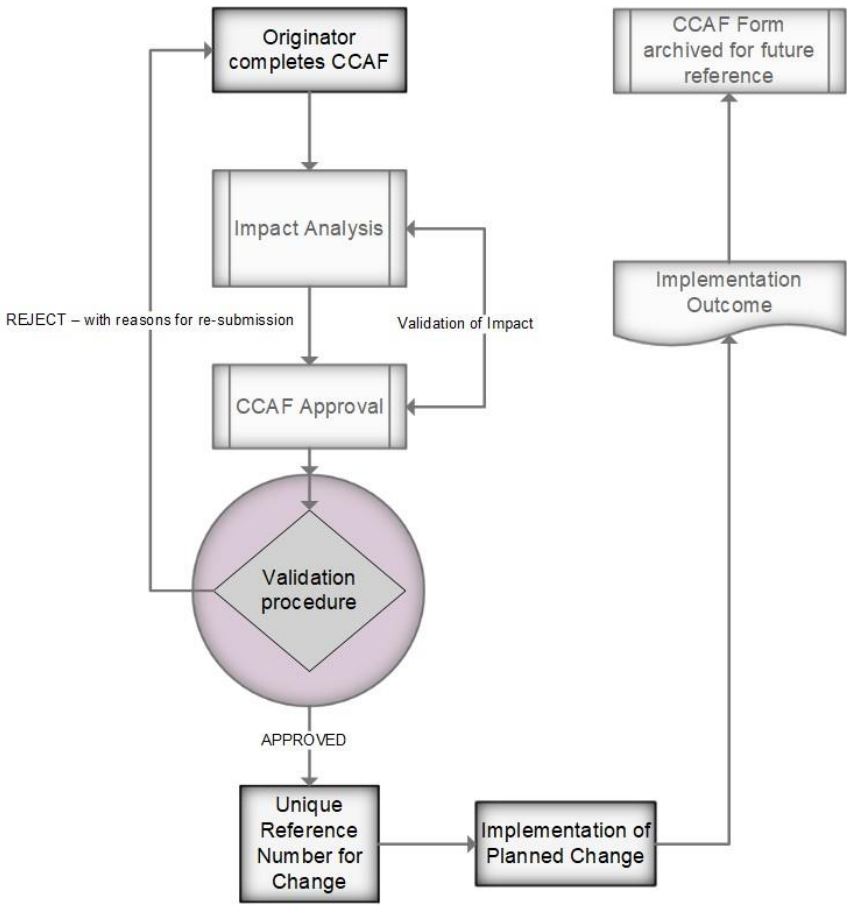


DIAGRAM 1 – PLANNED CHANGES WORKFLOW

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.

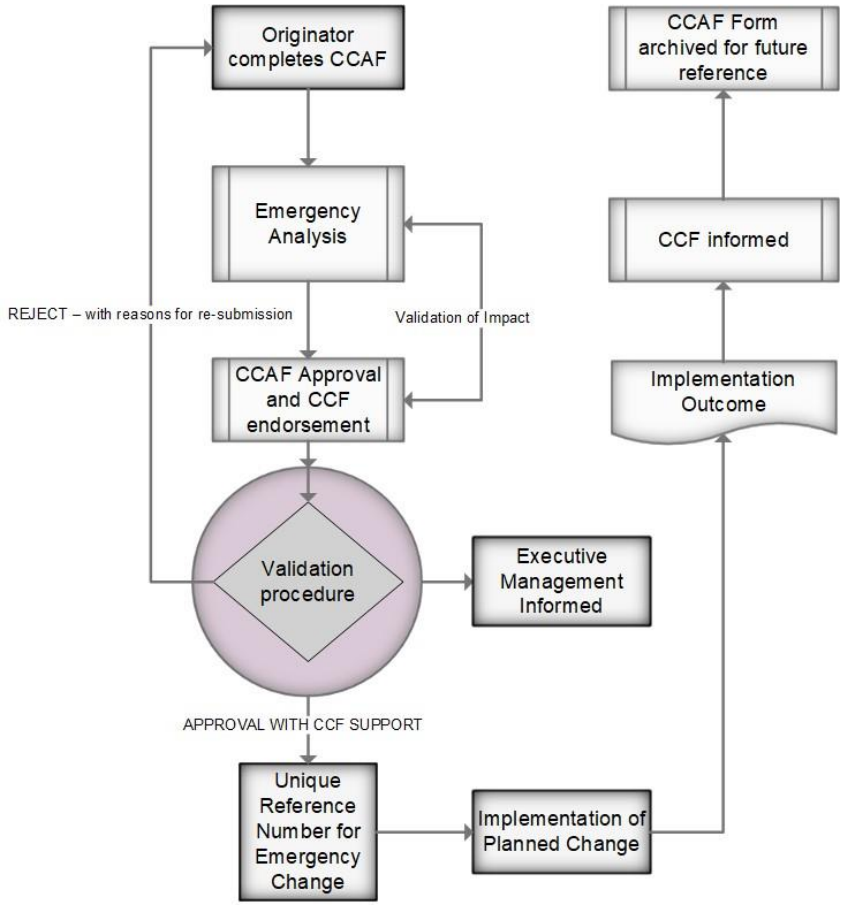


DIAGRAM 2 – EMERGENCY CHANGES WORKFLOW

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.

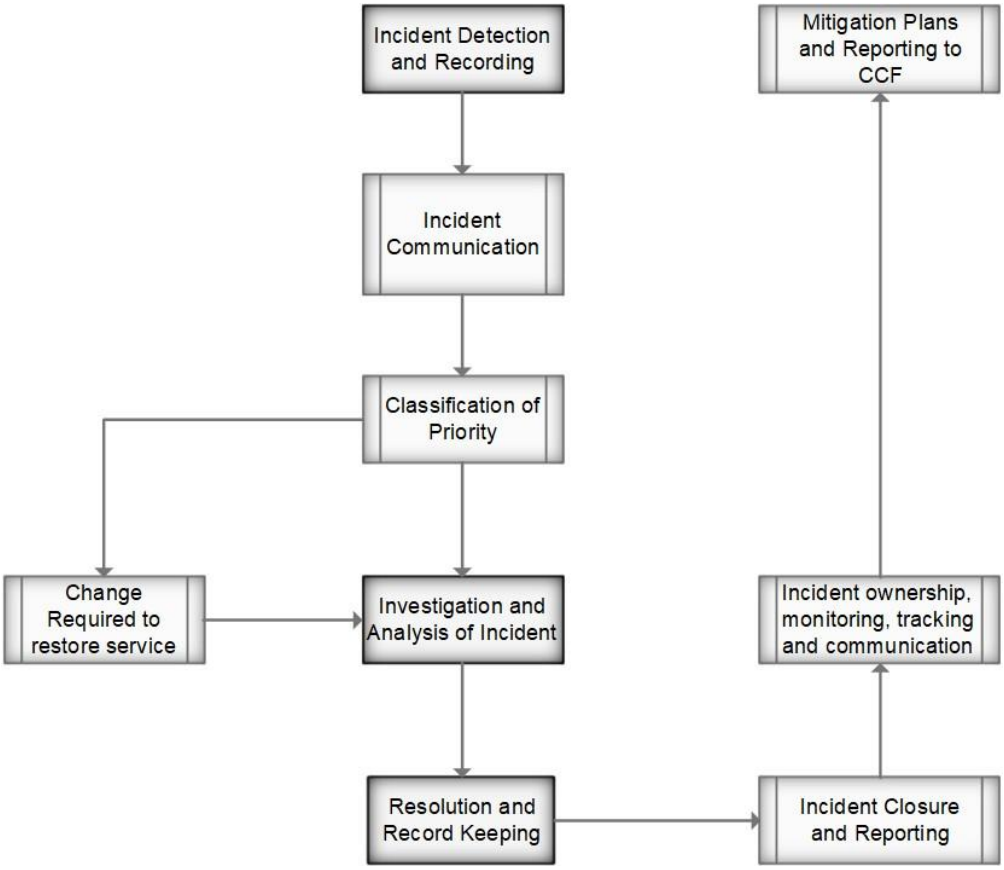


DIAGRAM 3 – INCIDENT MANAGEMENT WORKFLOW

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.

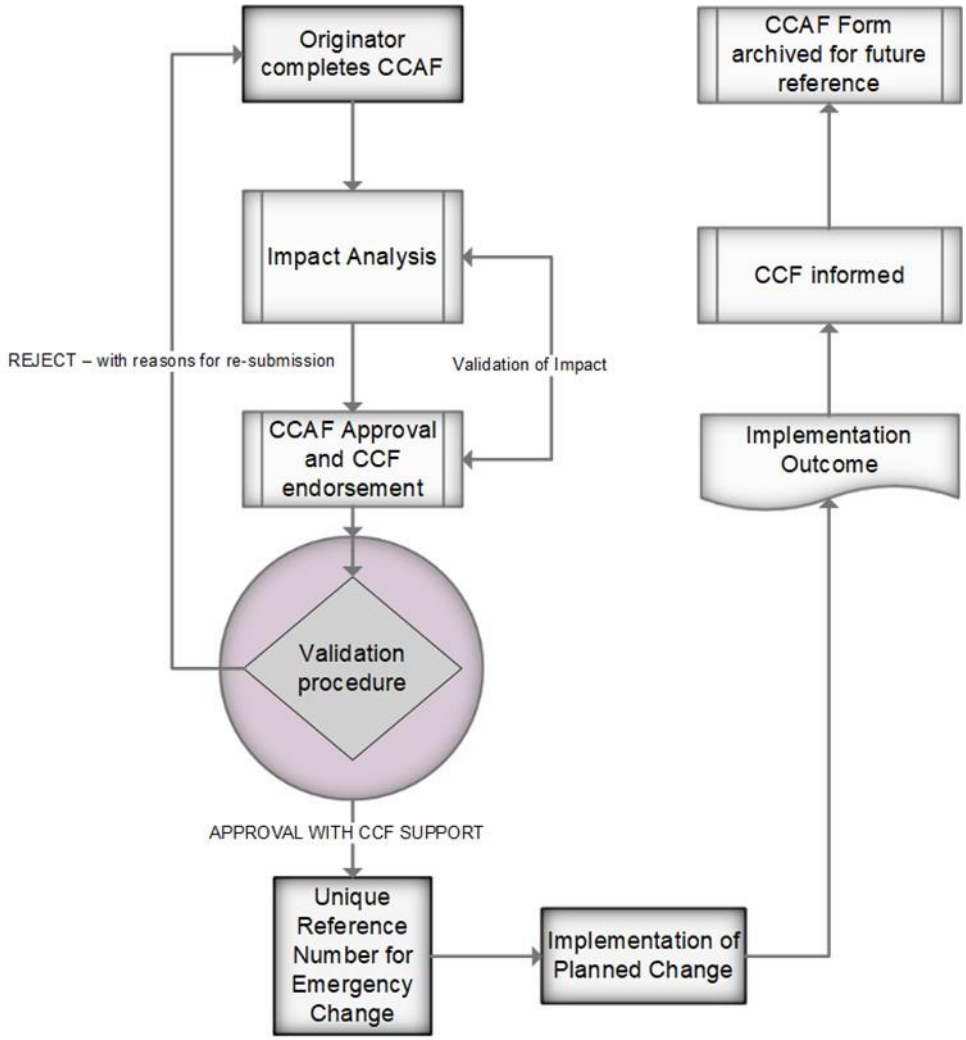


DIAGRAM 4 – MAJOR CHANGES WORKFLOW

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:

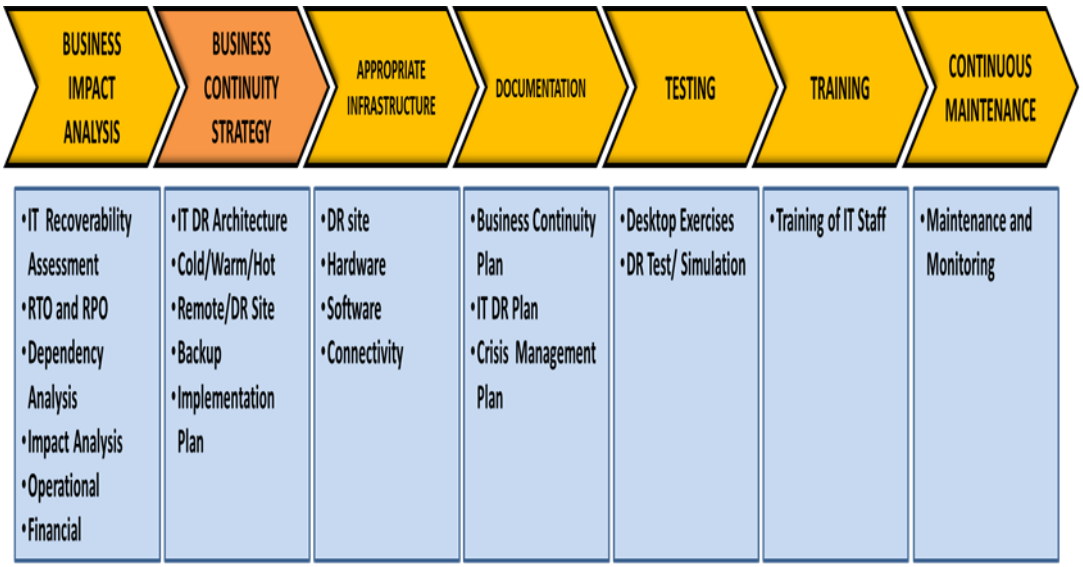


Figure 1: Methodology

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:

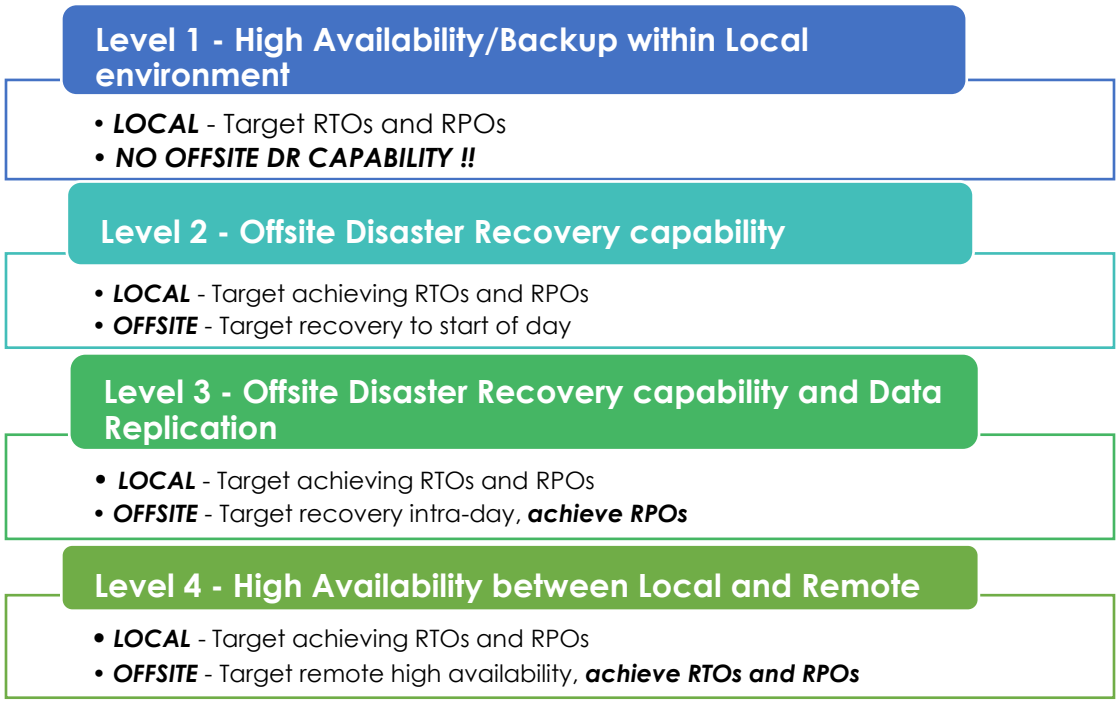


Figure 3: Levels of Resilience

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

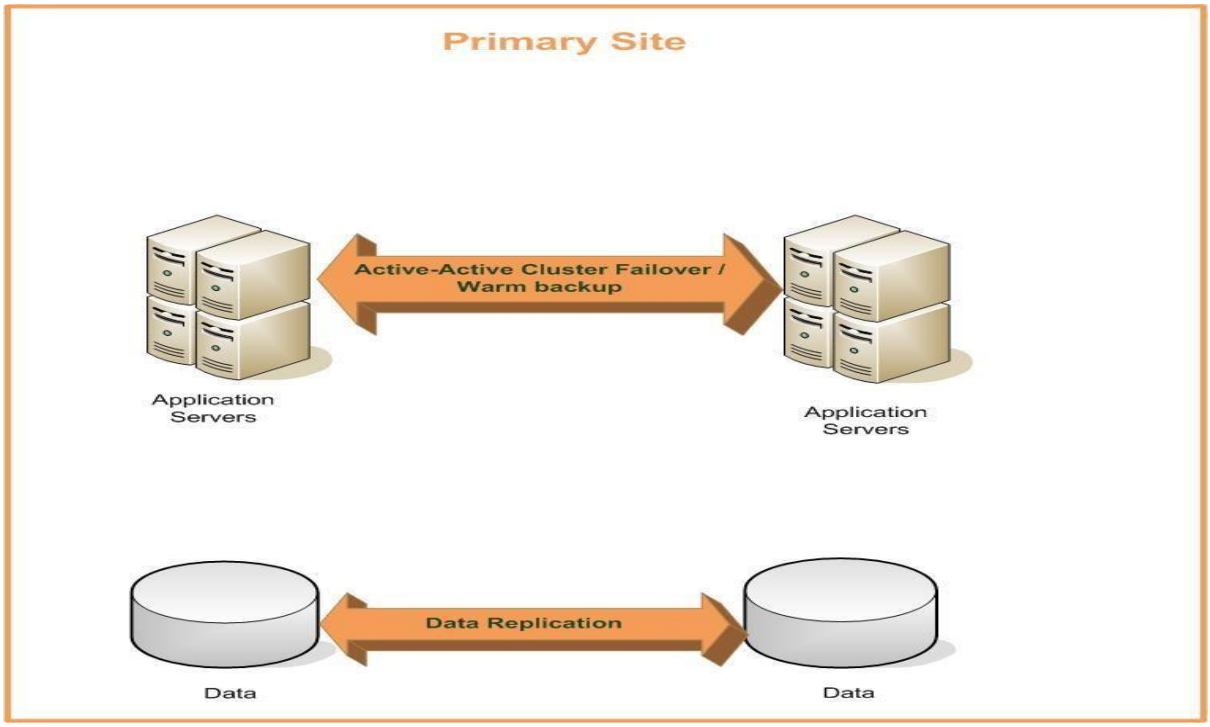


Figure 4: Level 1 Resilience

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

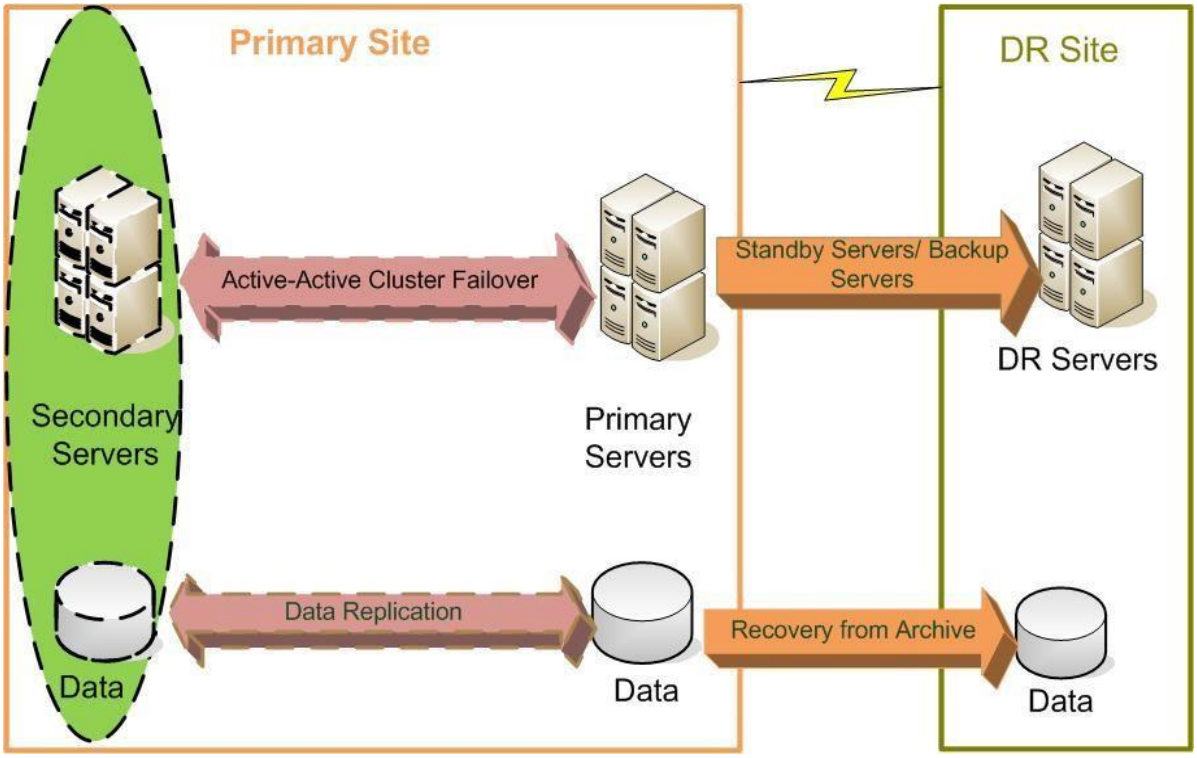


Figure 5: Level 2 Resilience

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

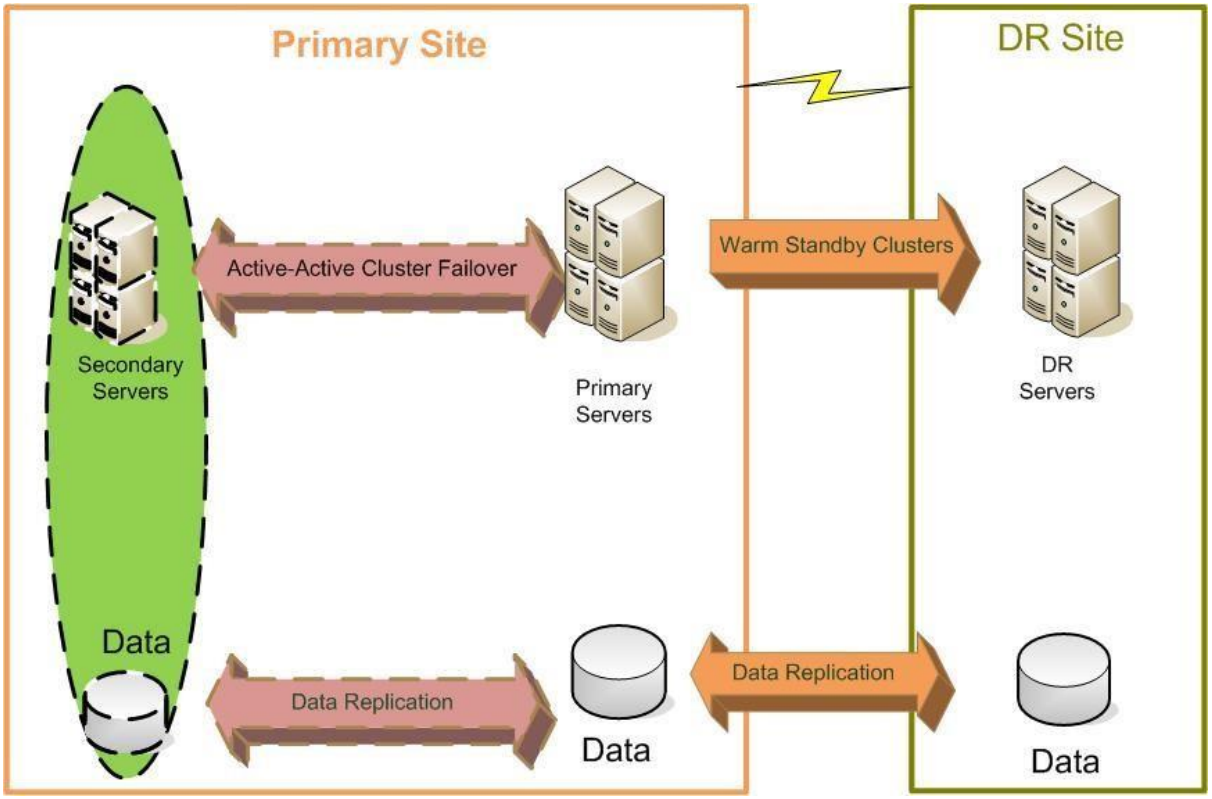


Figure 6: Level 3 Resilience

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

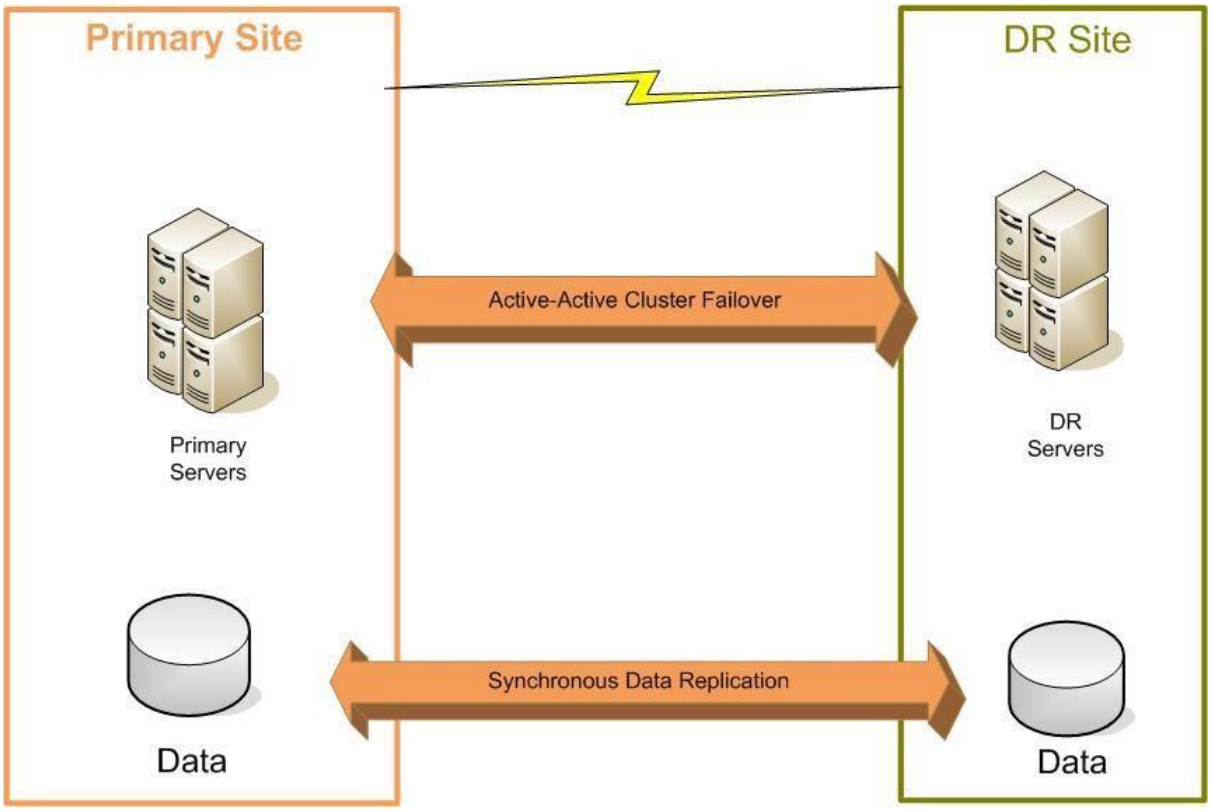


Figure 7: Level 4 resilience

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 aircooling 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 suppo rting 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 esse ntial 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 appli es 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 tocontinue to operate after a disaster has rendered any or all the systems inoperable.

2. AUDIENCE

The Disaster Recovery Champions and the associated teamsresponsible 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 c oordinate 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

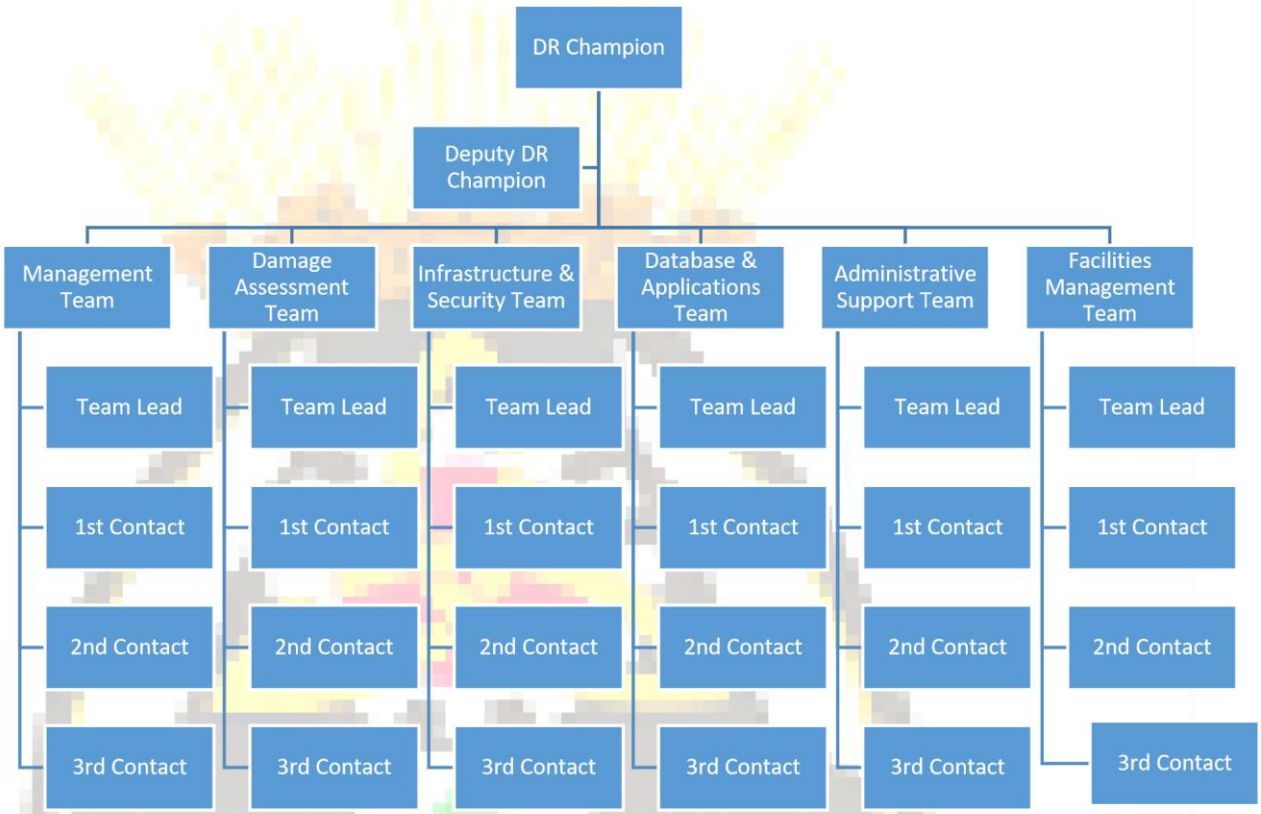
The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery.

The following teams have been developed and trained to respond t o 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 Lo cal Municipality computer systems environment and all applications. Members of the DRP team s include personnel who are also responsible for the daily operations and maintenance of Matjhabeng Local Municipality systems. The Damage Assessment team leader dir ects 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 t o 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 reco very 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 disa ster after effects, and execution phase activ ities are subsequently shut down. If the original system or facility is unrecoverable, this phase also involves rebuilding. Hence the reconstitution phas e 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 a t 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.

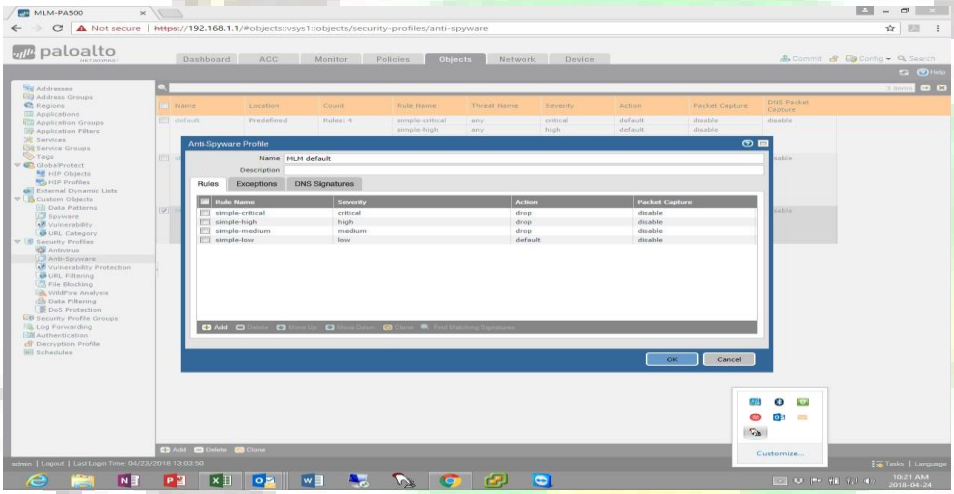
16. NETWORK MANAGEMENT SYSTEMS

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

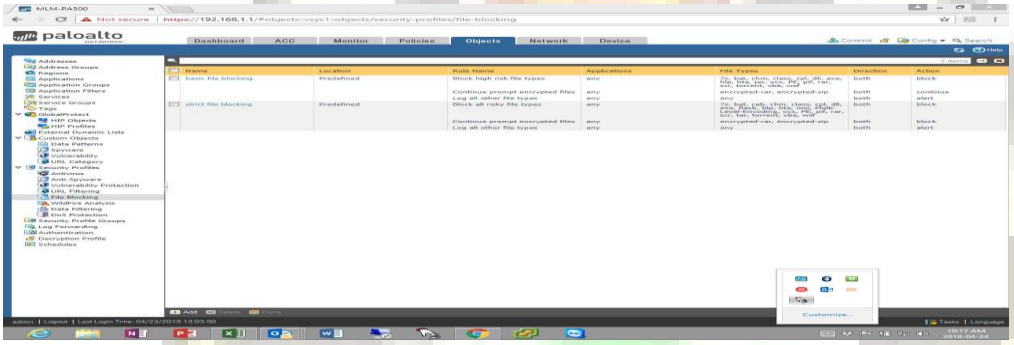
files, firewall systems administration procedural documentation files, and related files must be kept close to the firewall at all times.

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.

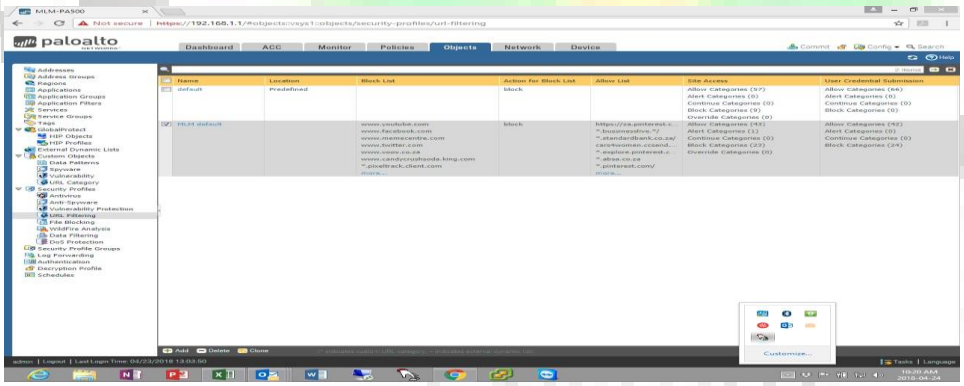


Objects and sites blocking, include

- 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

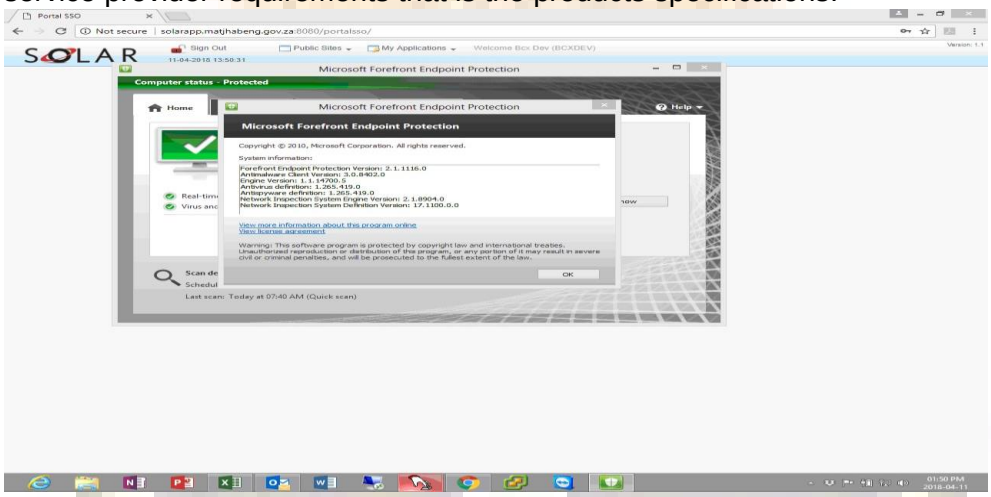
Firewalls must run on dedicated machines that perform no other services, such as acting as a mail server. Sensitive or critical MLM information must never be stored on a firewall. Such information may be held in buffers as it passes through a firewall. Firewalls must have only the bare minimum of operating 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 vendorprovided 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

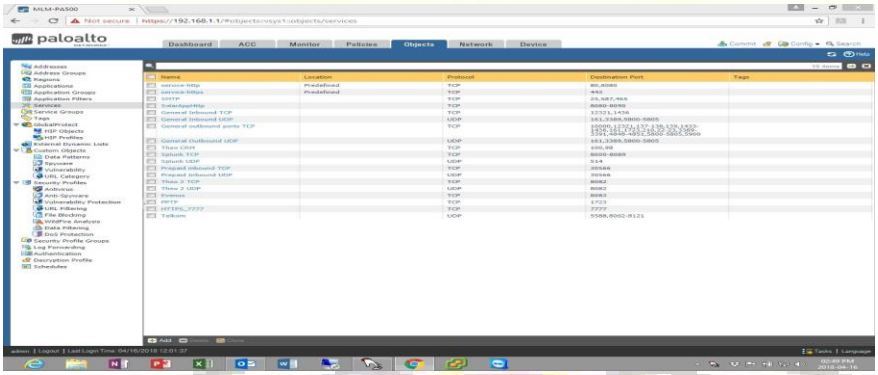
MLM staff members responsible for managing firewalls should stay current with information about firewall vulnerabilities. Any vulnerability that appears to affect MLM networks and systems must promptly be brought to the attention of the ICT Manager.

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

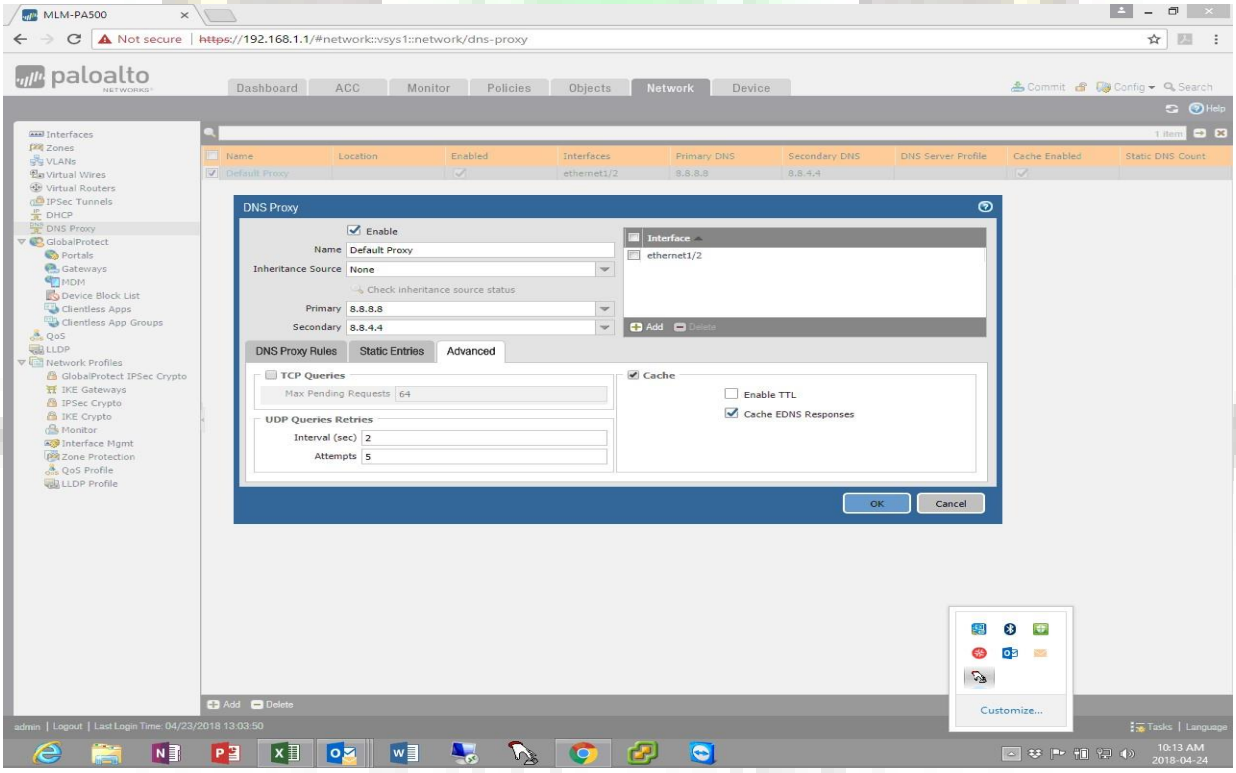
25. FIREWALL ACCESS MECHANISMS



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

LAPTOP POLICY & GUIDANCE

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 institute d 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 conf identiality, 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 switchedon. 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 Me eting.

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 po licy 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 I CT 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

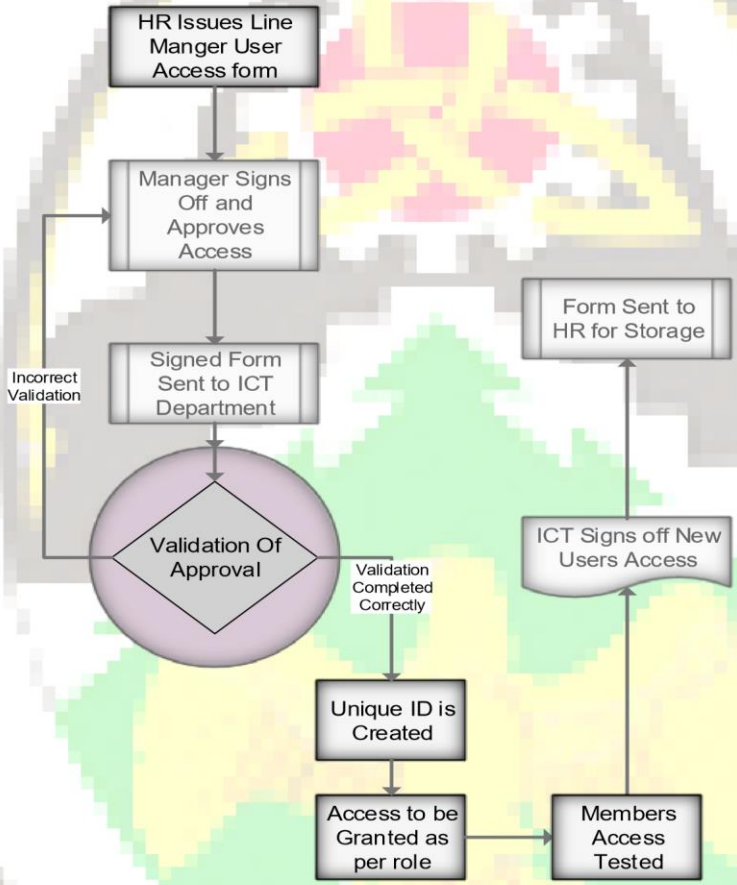
In accordance with the ICT Governance Policy, it is the responsibility of the Municipal Manager to determine the delegation of authority, personnel responsibilities and accountability to Management with regards to the Corporate Governance of ICT.

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.

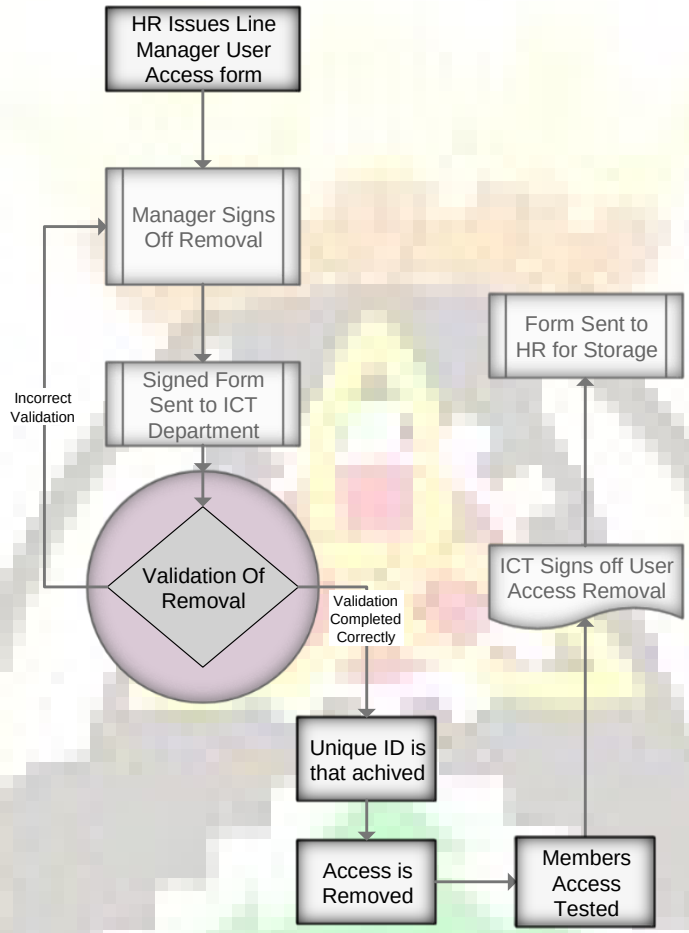


The unique ID must be associated with the HR and easy for members' recognition.
Examples:

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**

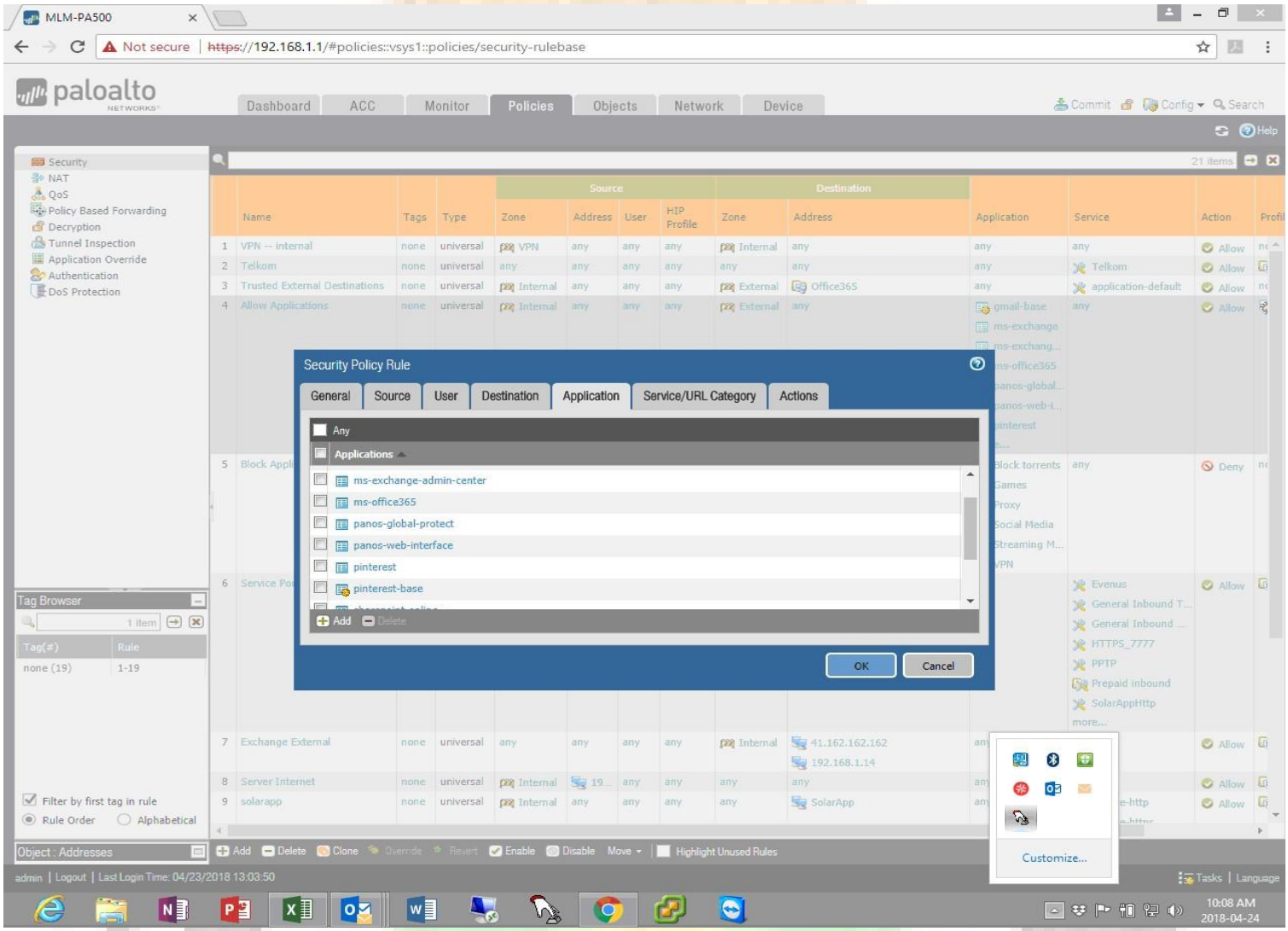
Restricted Access will fall on domains that have been block from accessing specific websites like for example:-

- 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 gove rns wireless device s 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, a ll 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 individu al 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 counc ilor/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 COUNCI LLORS 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 emp loyment 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 dep artment 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

SOLAR DISASTER RECOVERY GUIDE

MARCH 2019

Last Updated 28 March 2019

Table of Contents

Introduction

This document describes the procedure for disaster recovery for SolarDB in the event that the system goes down. This system holds all the Financial Information of the Matjhabeng Municipality.

Background

The Server Specifications for the SOLAR installation are:

Server Name: **SolarDb**

Hardware Specifications
VmWare
155935Mb Ram
2042MHz CPU
64bit
7.73 TB allocated space
Software Specifications
Windows Server 2012 R2 Std 64-bit
Solar DB system
SQL2012 Visual+
VmWare tools

Settings and Checklist

IP Addresses

- The IP Address for Production is: 192.168.1.20
- The IP Address for Backup is: 192.168.1.10 Veeam.

Port Numbers

Server and Database

- Server Logon is using the bcxdev user.

Change configuration checklist

✓ IP Address - 192.168.1.20

Connectivity

✓ Client to server.

Steps in switching to the backup

This will make the application available for use:

- Make sure Veeam server is running
- Setup server to perform backups, daily, weekly and Monthly.
- Also check backups in folder of the SolarDb server.

To revert back to the Production Machine / VM

- Do a backup of the database on the Backup Machine/VM that was running as the Production.
- Restore it onto the Production Machine/VM.
- From the Production Machine/VM follow the procedures for Database restore.
- Revert to the original IP address.
- Check connectivity and that the services are running.

APPENDIX A – DISASTER RECOVERY GLOSSARY OF TERMS

Term	Definition
Alert	Notification that a potential disaster situation is imminent exists or has occurred; usually includes a directive for personnel. To stand by for possible activation
Alternate Site	An alternate operating location to be used by business functions when the primary facilities are inaccessible. 1) Another location, computer centre or work area designated for recovery. 2) Location, other than the main facility, that can be used to conduct business functions. 3) A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster.
Alternate Work Area	Recovery environment complete with necessary infrastructure (desk, telephone, workstation, and associated hardware and equipment, communications, etc.)
Annual Loss Exposure/Expectancy (ALE)	A risk management method of calculating loss based on a value and level of frequency.
Application Recovery	The component of Disaster Recovery that deals specifically with the restoration of business system software and data after the processing platform has been restored or replaced.
Assembly Area	The designated area at which employees, visitors, and contractors assemble if evacuated from their building/site.
Asset	An item of property and/or component of a business activity/process owned by an organization. There are three types of assets: physical assets (e.g. buildings and equipment); financial assets (e.g. currency, bank deposits and shares) and non-tangible assets (e.g. goodwill, reputation)
Awareness	To create understanding of basic BCM issues and limitations. This will enable staff to recognise threats and respond accordingly. Examples of creating such awareness include distribution of posters and flyers targeted at company-wide audience or conducting specific business continuity briefings for executive management of the organization. Awareness is less formal than training and is generally targeted at all staff in the organization
Backlog	The effect on the business of a build-up of work that occurs as the result of a system or process being unavailable for an unacceptable period. A situation whereby a backlog of work requires more time to action than is available through normal working patterns.
Backup (Data)	A process by which data, electronic or paper-based, is copied in some form so as to be available and used if the original data from which it originated is lost, destroyed or corrupted.
Backup Generator	An independent source of power, usually fuelled by diesel or natural gas.
Battle Box	A container - often literally a box or brief case - in which data and information is stored so as to be immediately available post incident. Editor's Note: Electronic records held in a secure but accessible location on the internet are sometimes
Business Continuity	A program which develops, exercises and maintains plans to enable the organization to:-respond to a disruption with

Term	Definition
	minimum harm to life and resources;-recover, resume and restore functions within time frames which ensure continuing viability; and-provide crisis communications to all stakeholders. *Note: the program and its outputs: are based upon risk evaluation and impact assessment; and require management support, staff training and coordination with external agencies.*
Business Continuity Coordinator	A role within the BCM program that coordinates planning and implementation for overall recovery of an organization or unit(s).
Business Continuity Institute (BCI)	The Institute of professional Business Continuity Managers. Website www.thebci.org..
Business Continuity Management (BCM)	A holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats—if realized—might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities..
Business Continuity Management Process	The Business Continuity Institute's BCM Process provides guidance on good practices that cover the whole BCM Lifecycle and combines 5 key elements: 1) Understanding Your Business 2) BCM Strategies 3) Developing a BCM Response 4) Establishing a BCM Culture 5) Exercising, Maintenance and Audit
Business Continuity Management Program	An ongoing management and governance process supported by senior management and resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products/services through exercising, rehearsal, testing, training, maintenance and assurance.
Business Continuity Management Team	A group of individuals functionally responsible for directing the development and execution of the business continuity plan, as well as responsible for declaring a disaster and providing direction during the recovery process, both pre-disaster and post-disaster. Similar terms: disaster recovery management team, business recovery management team.
Business Continuity Maturity Model (BCMM)	A tool to measure the level and degree to which BCM activities have become standard and assured business practices within an organization.
Business Continuity Plan (BCP) Business Continuity Planning	A documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical products and services at an acceptable predefined level.
Business Continuity Plan Administrator	The designated individual responsible for plan documentation, maintenance, and distribution
Business Continuity Steering Committee	A top management group to give direction, advice, guidance and financial approval for the BCM programmes undertaken by the BCM Manager and various BC Coordinators.
Business Continuity Strategy	An approach by an organization that will ensure its recovery and continuity in the face of a disaster or other major outage. Plans

Term	Definition
	and methodologies are determined by the organization's strategy. There may be more than one solution to fulfil an organization's strategy. Examples: Internal or external hot-site, or cold-site, Alternate Work Area reciprocal agreement, Mobile Recovery, Quick Ship / Drop Ship, Consortium-based solutions, etc.
Business Continuity Team	Designated individuals responsible for developing, execution, rehearsals, and maintenance of the business continuity plan, including the processes and procedures. Similar terms: disaster recovery team, business recovery team, and recovery team.
Business Impact Analysis	A process designed to prioritize business functions by assessing the potential quantitative (financial) and qualitative (non-financial) impact that might result if an organization was to experience a business continuity event.
Business Interruption	Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations at an organization's location. Similar terms: outage, service interruption.
Business Interruption Insurance	Insurance coverage for disaster related expenses that may be incurred until operations are fully recovered after a disaster. Business interruption insurance generally provides reimbursement for necessary ongoing expenses during this shutdown, plus loss of net profits that would have been earned during the period of interruption, within the limits of the policy.
Business Recovery Coordinator	An individual or group designated to coordinate or control designated recovery processes or testing.
Business Recovery Team	A group responsible for: relocation and recovery of business unit operations at an alternate site following a business disruption; and subsequent resumption and restoration of those operations at an appropriate site.
Business Recovery Timeline	The approved sequence of activities, required to achieve stable operations following a business interruption. This timeline may range from minutes to weeks, depending upon the recovery requirements and methodology.
Business Unit Recovery	A component of Business Continuity which deals specifically with the recovery of a key function or department in the event of a disaster.
Call Tree	A document that graphically depicts the calling responsibilities and the calling order used to contact management, employees, customers, vendors, and other key contacts in the event of an emergency, disaster, or severe outage situation.
Cascade System	A system whereby one person or organization calls out/contacts others who in turn initiate further call-outs/contacts as necessary.
Checklist	a) Tool to remind and /or validate that tasks have been completed and resources are available, to report on the status of recovery. b) A list of items (names or tasks etc.) to be checked or consulted.
Checklist Exercise	A method used to exercise a completed disaster recovery plan. This type of exercise is used to determine if the information such

Term	Definition
	as phone numbers, manuals, equipment, etc. in the plan is accurate and current.
Cold Site	An alternate facility that already has in place the environmental infrastructure required to recover critical business functions or information systems, but does not have any pre-installed computer hardware, telecommunications equipment, communication lines, etc. These must be provisioned at time of disaster.
Command Centre	The facility used by a Crisis Management Team after the first phase of a plan invocation. An organization must have a primary and secondary location for a command centre in the event of one being unavailable. It may also serve as a reporting point for deliveries, services, press and all external contacts.
Command, Control and Coordination	A Crisis Management process. Command means the authority for an organization or part of an organization to direct the actions of its own resources (both personnel and equipment). Control means the authority to direct strategic, tactical and operational operations in order to complete an assigned function. This includes the ability to direct the activities of others engaged in the completion of that function, i.e. the crisis as a whole or a function within the crisis management process. The control of an assigned function also carries with it the responsibility for the health and safety of those involved. Coordination means the integration of the expertise of all the agencies/roles involved with the objective of effectively and efficiently bringing the crisis to a successful conclusion.
Communications Recovery	The component of Disaster Recovery which deals with the restoration or rerouting of an organization's telecommunication network, or its components, in the event of loss.
Contact List	A list of team members and/or key personnel to be contacted including their backups. The list will include the necessary contact information (i.e. home phone, pager, cell, etc.) and in many cases it is considered confidential.
Contingency Plan	A plan used by an organization or business unit to respond to a specific systems failure or disruption of operations.
Contingency Planning	Process of developing advanced arrangements and procedures that enable an organization to respond to an undesired event that negatively impacts the organization.
Continuity Of Operations Plan (COOP)	A COOP provides guidance on the system restoration for emergencies, disasters, mobilization, and for maintaining a state of readiness to provide the necessary level of information processing support commensurate with the mission requirements/priorities identified by the respective functional proponent. The Federal Government and its supporting agencies traditionally use this term to describe activities otherwise known as Disaster Recovery, Business Continuity, Business Resumption, or Contingency Planning.
Continuous Availability	A system or application that supports operations which continue with little to no noticeable impact to the user. For instance, with

Term	Definition
	continuous availability, the user will not have to re-log in, or to re-submit a partial or whole transaction.
Continuous Operations	The ability of an organization to perform its processes without interruption.
Corporate Governance	The system/process by which the directors and officers of an organization are required to carry out and discharge their legal, moral and regulatory accountabilities and responsibilities.
Corporate Risk	A category of risk management that looks at ensuring an organization meets its corporate governance responsibilities takes appropriate actions and identifies and manages emerging risks.
Cost Benefit Analysis	A process (after a BIA and risk assessment) that facilitates the financial assessment of different strategic BCM options and balances the cost of each option against the perceived savings.
Crisis	A critical event, which, if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation, or ability to operate. Or, an occurrence and/or perception that threatens the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an organization.
Crisis Management	The overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, and ability to operate.
Crisis Management Team	A team consisting of key executives, key role players (i.e., media representative, legal counsel, facilities manager, disaster recovery coordinator, etc.), and the appropriate business owners of critical functions who are responsible for recovery operations during a crisis.
Critical Business Functions	The critical operational and/or business support functions that could not be interrupted or unavailable for more than a mandated or predetermined timeframe without significantly jeopardizing the organization. An example of a business function is a logical grouping of processes/activities that produce a product and/or service such as Accounting, Staffing, Customer Service, etc.
Critical Data Point	The point in time to which data must be restored in order to achieve recovery objectives.
Critical Infrastructure	Physical assets whose incapacity or destruction would have a debilitating impact on the economic or physical security of an organization, community, nation, etc.
Critical Service	A service without which a building would be "disabled". Often applied to the utilities (water, gas, electric, etc.) it may also include standby power systems, environmental control systems or communication networks
Damage Assessment	The process of assessing damage to computer hardware, vital records, office facilities, etc. and determining what can be salvaged or restored and what must be replaced following a disaster.

Term	Definition
Data Backup Strategies	Data backup strategies will determine the technologies, media and offsite storage of the backups necessary to meet an organization's data recovery and restoration objectives.
Data Backups	The copying of production files to media that can be stored both on and/or offsite and can be used to restore corrupted or lost data or to recover entire systems and databases in the event of a disaster.
Data Centre Recovery	The component of Disaster Recovery which deals with the restoration of data centre services and computer processing capabilities at an alternate location and the migration back to the production site.
Data Mirroring	A process whereby critical data is replicated to another device.
Data Protection	Process of ensuring confidentiality, integrity and availability of data
Data Recovery	The restoration of computer files from backup media to restore programs and production data to the state that existed at the time of the last safe backup.
Database Replication	The partial or full duplication of data from a source database to one or more destination databases.
Declaration	A formal announcement by pre-authorized personnel that a disaster or severe outage is predicted or has occurred and that triggers pre-arranged mitigating actions (e.g., a move to an alternate site.)
Denial of Access	The inability of an organization to access and/or occupy its normal working environment.
Dependency	The reliance or interaction of one activity or process upon another.
Desk Check	One method of validating a specific component of a plan. Typically, the owner of the component reviews it for accuracy and completeness and signs off.
Desktop Exercise	See: Table Top Exercise.
Disaster	A sudden, unplanned catastrophic event causing unacceptable damage or loss. 1) An event that compromises an organization's ability to provide critical functions, processes, or services for some unacceptable period of time 2) An event where an organization's management invokes their recovery plans.
Disaster Recovery	The technical aspect of business continuity. The collection of resources and activities to re-establish information technology services (including components such as infrastructure, telecommunications, systems, applications and data) at an alternate site following a disruption of IT services. Disaster recovery includes subsequent resumption and restoration of those operations at a more permanent site.
Disaster Recovery Plan	The management approved document that defines the resources, actions, tasks and data required to manage the technology recovery effort. Usually refers to the technology recovery effort. This is a component of the Business Continuity Management Program.
Disaster Recovery Planning	The technical component of business continuity planning

Term	Definition
DRI International	DRI International is a non-profit organization that offers premier educational and certification programs globally, for those practitioners within the Continuity Management field.
Drop Ship	A strategy for a) Delivering equipment, supplies, and materials at the time of a business continuity event or exercise. b) Providing replacement hardware within a specified time period via prearranged contractual arrangements with an equipment supplier at the time of a business continuity event.
Electronic Vaulting	Electronic transmission of data to a server or storage facility.
Emergency	An unexpected or impending situation that may cause injury, loss of life, destruction of property, or cause the interference, loss, or disruption of an organization's normal business operations to such an extent that it poses a threat.
Emergency Control Centre (ECC)	The Command Centre used by the Crisis Management Team during the first phase of an event. An organization should have both primary and secondary locations for an ECC in case one of them becomes unavailable/inaccessible. It may also serve as a reporting point for deliveries, services, press and all external contacts.
Emergency Coordinator	The person designated to plan, exercise, and implement the activities of sheltering in place or the evacuation of occupants of a site with the first responders and emergency services agencies.
Emergency Operations Centre (EOC)	The physical and/or virtual location from which strategic decisions are made and all activities of an event/incident/crisis are directed, coordinated and monitored. *Note: EOC is different from Command Centre.*
Emergency Preparedness	The capability that enables an organization or community to respond to an emergency in a coordinated, timely, and effective manner to prevent the loss of life and minimize injury and property damage.
Emergency Procedures	A documented list of activities to commence immediately to prevent the loss of life and minimize injury and property damage.
Emergency Response	The immediate reaction and response to an emergency situation commonly focusing on ensuring life safety and reducing the severity of the incident.
Emergency Response Plan	A documented plan usually addressing the immediate reaction and response to an emergency situation
Emergency Response Procedures	The initial response to any event and is focused upon protecting human life and the organization's assets.
Emergency Response Team (ERT)	Qualified and authorized personnel who have been trained to provide immediate assistance.
Enterprise Risk Management	ERM includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a © BCI 2011

Term	Definition
	Page 22 Dictionary of Business Continuity Management Terms TERM DEFINITION REFERENCES response strategy, and monitoring progress. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall..
Escalation	Infrastructure services without which a building or area would be considered disabled and unable to provide normal operating services; typically includes utilities (water, gas, electricity, telecommunications), and may also include standby power systems or environmental control systems.
Evacuation	The movement of employees, visitors and contractors from a site and/or building to a safe place (assembly area) in a controlled and monitored manner at time of an event.
Event	Any occurrence that may lead to a business continuity incident.
Executive / Management Succession Plan	A predetermined plan for ensuring the continuity of authority, decision-making, and communication in the event that key members of executive management unexpectedly become incapacitated.
Exercise	A people focused activity designed to execute business continuity plans and evaluate the individual and/or organization performance against approved standards or objectives. Exercises can be announced or unannounced, and are performed for the purpose of training and conditioning team members, and validating the business continuity plan. Exercise results identify plan gaps and limitations and are used to improve and revise the Business Continuity Plans. Types of exercises include: Table Top Exercise, Simulation Exercise, Operational Exercise, Mock Disaster, Desktop Exercise, and Full Rehearsal.
Exercise Auditor	An appointed role that is assigned to assess whether the exercise aims / objectives are being met and to measure whether activities are occurring at the right time and involve the correct people to facilitate their achievement. The exercise auditor is not responsible for the mechanics of the exercise. This independent role is crucial in the subsequent debriefing.
Exercise Controller	See Exercise Owner
Exercise Coordinator	They are responsible for the mechanics of running the exercise. The Coordinator must lead the exercise and keep it focused within the predefined scope and objectives of the exercise as well as on the disaster scenario. The Coordinator must be objective and not influence the outcome. They perform the coordination to make sure appropriate exercise participants have been identified and that exercise scripts have been prepared before, utilized during, and updated after the exercise.
Exercise Observer	An exercise observer has no active role within the exercise but is present for awareness and training purposes. An exercise observer might make recommendations for procedural improvements.
Exercise Owner	An appointed role that has total management oversight and control of the exercise and has the authority to alter the exercise

Term	Definition
	plan. This includes early termination of the exercise for reasons of safety or the aims / objectives of the exercise cannot be met due to an unforeseen or other internal or external influence.
Exercise Plan	A plan designed to periodically evaluate tasks, teams, and procedures that are documented in business continuity plans to ensure the plan's viability. This can include all or part of the BC plan, but should include mission critical components.
Exercise Script	A set of detailed instructions identifying information necessary to implement a predefined business continuity event scenario for evaluation purposes.
Exposure	The potential susceptibility to loss; the vulnerability to a particular risk.
First Responder	A member of an emergency service who is first on the scene at a disruptive incident. This would normally be police, fire or ambulance personnel.
Floor Warden	Person responsible for ensuring that all employees, visitors and contractors evacuate a floor within a specific site.
Full Rehearsal	An exercise that simulates a Business Continuity event where the organization or some of its component parts are suspended until the exercise is completed.
Gap Analysis	A detailed examination to identify risks associated with the differences between Business/Operations requirements and the current available recovery capabilities.
Governance, Risk and Compliance (GRC)	GRC is the umbrella term covering an organization's approach across these three areas. Being closely related concerns, governance, risk and compliance activities are increasingly being integrated and aligned to some extent in order to avoid conflicts, wasteful overlaps and gaps. While interpreted differently in various organizations, GRC typically encompasses activities such as corporate © BCI 2011 Page 25 Dictionary of Business Continuity Management Terms TERM DEFINITION REFERENCES governance, enterprise risk management (ERM) and corporate compliance with applicable laws and regulations.
Hardening	The process of making something more secure, resistant to attack, or less vulnerable.
Health and Safety	The process by which the wellbeing of all employees, contractors, visitors and the public is safeguarded. All business continuity plans and planning must be cognizant of H&S statutory and regulatory requirements and legislation. Health and Safety considerations should be reviewed during the Risk assessment.
High-Availability	Systems or applications requiring a very high level of reliability and availability. High availability systems typically operate 24×7 and usually require built-in redundancy to minimize the risk of downtime due to hardware and/or telecommunication failures.
High-Risk Areas	Areas identified during the risk assessment that are highly susceptible to a disaster situation or might be the cause of a significant disaster."

Term	Definition
Hot site	An alternate facility that already has in place the computer, telecommunications, and environmental infrastructure required to recover critical business functions or information systems.
Human Continuity	The ability of an organization to provide support for its associates and their families before, during, and after a business continuity event to ensure a viable workforce. This involves pre planning for potential psychological responses, occupational health and employee assistance programs, and employee communications.
Human Threats	Possible disruptions in operations resulting from human actions as identified during the risk assessment. (i.e., disgruntled employee, terrorism, blackmail, job actions, riots, etc.)
ICT Continuity	Capability of the organization to plan for and respond to incidents and disruptions in order to continue ICT services at an acceptable level.
ICT Disaster Recovery (ICT DR)	The ability of the ICT elements of an organization to support its critical business functions to acceptable levels within a pre-determined period of time following a disruption.
ICT Disaster Recovery Plan (ICT DRP)	A clearly defined and documented plan which recovers ICT capabilities when a disruption occurs
Impact	The effect, acceptable or unacceptable, of an event on an organization. The types of business impact are usually described as financial and non-financial and are further divided into specific types of impact.
Incident	An event which is not part of a standard operating business which may impact or interrupt services and, in some cases, may lead to disaster.
Incident Command System (ICS)	Combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure with responsibility for the command, control, and coordination of assigned resources to effectively direct and control the response and recovery to an incident. The flexible design of the ICS allows its span of control to expand or contract as the scope of the situation changes
Incident Management	The process by which an organization responds to and controls an incident using emergency response procedures or plans.
Incident Manager	Commands the local emergency operations centre (EOC) reporting up to senior management on the recovery progress. Has the authority to invoke the recovery plan
Incident Response	The response of an organization to a disaster or other significant event that may significantly impact the organization, its people, or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan, performing damage assessment, and any other measures necessary to bring an organization to a more stable status.
Information Security	The securing or safeguarding of all sensitive information, electronic or otherwise, which is owned by an organization.
Infrastructure	The underlying foundation, basic framework, or interconnecting structural elements that support an organization.

Term	Definition
Integrated Exercise	An exercise conducted on multiple interrelated components of a Business Continuity Plan, typically under simulated operating conditions. Examples of interrelated components may include interdependent departments or interfaced systems.
Integrated Test	See integrated exercise
Interim Site	A temporary location used to continue performing business functions after vacating a recovery site and before the original or new home site can be occupied. Move to an interim site may be necessary if ongoing stay at the recovery site is not feasible for the period of time needed or if the recovery site is located far from the normal business site that was impacted by the disaster. An interim site move is planned and scheduled in advance to minimize disruption of business processes; equal care must be given to transferring critical functions from the interim site back to the normal business site.
Internal Hot site	A fully equipped alternate processing site owned and operated by the organization.
ISO 27000 series	ISO standards for Information Security, one section of which provides guidance on Business Continuity. There are three standards ISO 27001, ISO 27002 and ISO 27003. They should not be viewed as full BCM standards.
ISO 31000	ISO standard for Risk Management.
Key Tasks	Priority procedures and actions in a Business Continuity Plan that must be executed within the first few minutes/hours of the plan invocation.
Lead Time	The time it takes for a supplier to make equipment, services, or supplies available after receiving an order. Business continuity plans should try to minimize lead time by creating service level agreements (SLA) with suppliers or alternate suppliers in advance of a Business Continuity event rather than relying on the suppliers' best efforts.
Loss	Unrecoverable resources that are redirected or removed as a result of a Business Continuity event. Such losses may be loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability.
Manual Procedures	An alternative method of working following a loss of IT systems. As working practices rely more and more on computerized activities, the ability of an organization to fall-back to manual alternatives lessens. However, temporary measures and methods of working can help mitigate the impact of a business continuity event and give staff a feeling of doing something.
Maximum Tolerable Period of Disruption (MTPD or MTPoD)	The duration after which an organization's viability will be irrevocably threatened if a product or service delivery cannot be resumed.
Maximum Tolerable Period of Downtime.	Maximum Tolerable Period of Downtime.
Minimum Business Continuity Objective (MBCO)	Minimally acceptable collection of business continuity services and/or products that is acceptable to an organization or industry to achieve its business objectives that can be influenced or dictated by regulation or legislation level of business continuity.

Term	Definition
Mission-Critical Activities	The critical operational and/or business support activities (either provided internally or outsourced) required by the organization to achieve its objective(s) i.e. services and/or products.
Mission-Critical Application	Applications that support business activities or processes that could not be interrupted or unavailable for 24 hours or less without significantly jeopardizing the organization.
Mitigation	Limitation of any negative consequence of a particular incident.
Mobilization	The activation of the recovery organization in response to a disaster declaration.
Mock Disaster	One method of exercising teams in which participants are challenged to determine the actions they would take in the event of a specific disaster scenario. Mock disasters usually involve all, or most, of the applicable teams. Under the guidance of exercise coordinators, the teams walk through the actions they would take per their plans, or simulate performance of these actions. Teams may be at a single exercise location, or at multiple locations, with communication between teams simulating actual 'disaster mode' communications. A mock disaster will typically operate on a compressed timeframe representing many hours, or even days.
Network Outage	An interruption of voice, data, or IP network communications.
Off-Site Storage	Any place physically located a significant distance away from the primary site, where duplicated and vital records (hard copy or electronic and/or equipment) may be stored for use during recovery.
Operational Risk	The risk of loss resulting from inadequate or failed procedures and controls. This includes loss from events related to technology and infrastructure, failure, business interruptions, staff related problems, and from external events such as regulatory changes
Orderly Shutdown	The actions required to rapidly and gracefully suspend a business function and/or system during a disruption.
Outage	The interruption of automated processing systems, infrastructure, support services, or essential business operations, which may result, in the organizations inability to provide services for some period of time.
Peer Review	A review of a specific component of a plan by personnel (other than the owner or author) with appropriate technical or business knowledge for accuracy and completeness.
Plan Maintenance	The management process of keeping an organization's Business continuity management plans up to date and effective. Maintenance procedures are a part of this process for the review and update of the BC plans on a defined schedule. Maintenance procedures are a part of this process.
Preventative Measures	Controls aimed at deterring or mitigating undesirable events from taking place.
Qualitative Assessment	The process for evaluating a business function based on observations and does not involve measures or numbers. Instead, it uses descriptive categories such as customer service, regulatory requirements, etc. to allow for refinement of the

Term	Definition
	quantitative assessment. This is normally done during the BIA phase of planning.
Quantitative Assessment	The process for placing value on a business function for risk purposes. It is a systematic method that evaluates possible financial impact for losing the ability to perform a business function. It uses numeric values to allow for prioritizations. This is normally done during the BIA phase of planning.
Quick Ship	See Drop Ship.
Recoverable Loss	Financial losses due to an event that may be reclaimed in the future, e.g. through insurance or litigation. This is normally identified in the Risk Assessment or BIA.
Recovery	Implementing the prioritized actions required to return the processes and support functions to operational stability following an interruption or disaster.
Recovery Management Team	See: Business Continuity Management (BCM) Team.
Recovery Period	The time period between a disaster and a return to normal functions, during which the disaster recovery plan is employed.
Recovery Point Objective (RPO)	The point in time to which data is restored and/or systems are recovered after an outage. *Note: RPO is often used as the basis for developing backup strategies and determining the amount of data that may require recreation after systems have been recovered. RPO for applications can be enumerated in business time (i.e., "8 business hours" after a Sunday disaster restores to close of business Thursday) or elapsed time, but is always measured in terms of time before a disaster. RPO for systems typically must be established at time of disaster as a specific point in time (e.g., end of previous day's processing) or software version/release.*
Recovery Services Agreement / Contract	A contract with an external organization guaranteeing the provision of specified equipment, facilities, or services, usually within a specified time period, in the event of a business interruption. A typical contract will specify a monthly subscription fee, a declaration fee, usage costs, method of performance, amount of test time, termination options, penalties and liabilities, etc.
Recovery Site	A designated site for the recovery of business unit, technology, or other operations, which are critical to the enterprise.
Recovery Strategy	See business continuity strategy
Recovery Teams	A structured group of teams ready to take control of the recovery operations if a disaster should occur.
Recovery Time Capability (RTC) **Recovery Time Objective (RTO)**	The demonstrated amount of time in which systems, applications and/or functions have been recovered, during an exercise or actual event, at the designated recovery/alternate location (physical or virtual). As with RTO, RTC includes assessment, execution and verification activities. RTC and RTO are compared during gap analysis. The period of time within which systems, applications, or functions must be recovered after an outage. RTO includes the time required for: assessment, execution and verification. RTO may be

Term	Definition
	enumerated in business time (e.g. one business day) or elapsed time (e.g. 24 elapsed hours). *Notes: Assessment includes the activities which occur before or after an initiating event, and lead to confirmation of the execution priorities, time line and responsibilities, and a decision regarding when to execute.* *Execution includes the activities related to accomplishing the pre-planned steps required within the phase to deliver a function, system or application in a new location to its owner.* *Verification includes steps taken by a function, system or application owner to ensure everything is in readiness to proceed to live operations.*
Recovery Timeline	The sequence of recovery activities, or critical path, which must be followed to resume an acceptable level of operation following a business interruption. The timeline may range from minutes to weeks, depending upon the recovery requirements and methodology.
Residual Risk	The level of risk remaining after all cost-effective actions have been taken to lessen the impact, probability and consequences of a specific risk or group of risks, subject to an organization's risk appetite.
Resilience	The ability of an organization to absorb the impact of a business interruption, and continue to provide a minimum acceptable level of service.
Resilient	The process and procedures required to maintain or recover critical services such as “remote access” or “end-user support” during a business interruption.
Response	The reaction to an incident or emergency to assess the damage or impact and to ascertain the level of containment and control activity required. In addition to addressing matters of life safety and evacuation, Response also addresses the policies, procedures and actions to be followed in the event of an emergency.
Restoration	Process of planning for and/or implementing procedures for the repair of hardware, relocation of the primary site and its contents, and returning to normal operations at the permanent operational location.
Resumption	The process of planning for and/or implementing the restarting of defined business processes and operations following a disaster. This process commonly addresses the most critical business functions within BIA specified timeframes.
Risk	Potential for exposure to loss which can be determined by using either qualitative or quantitative measures.

Term	Definition
Risk Assessment / Analysis	Process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.
Risk Avoidance	An informed decision to not become involved in or to withdraw from a risk situation.
Risk Categories	Risks of similar types are grouped together under key headings, otherwise known as 'risk categories'. These categories include reputation, strategy, financial, investments, operational infrastructure, business, regulatory compliance, Outsourcing, people, technology and knowledge.
Risk Controls	All methods of reducing the frequency and/or severity of losses including exposure avoidance, loss prevention, loss reduction, segregation of exposure units and non-insurance transfer of risk
Risk Management	The culture, processes and structures that are put in place to effectively manage potential negative events. As it is not possible or desirable to eliminate all risk, the objective is to reduce risks to an acceptable level
Risk Reduction	A selective application of appropriate techniques and management principles to reduce either probability of an occurrence or its impact, or both.
Risk Transfer	A common technique used by Risk Managers to address or mitigate potential exposures of the organization. A series of techniques describing the various means of addressing risk through insurance and similar products.
Risk Treatment	Selection and implementation of measures to modify risk.
Roll Call	The process of identifying that all employees, visitors and contractors have been safely evacuated and accounted for following an evacuation of a building or site.
Salvage & Restoration	The act of conducting a coordinated assessment to determine the appropriate actions to be performed on impacted assets. The assessment can be coordinated with Insurance adjusters, facilities personnel, or other involved parties. Appropriate actions may include: disposal, replacement, reclamation, refurbishment, recovery or receiving compensation for unrecoverable organizational assets.
Security Review	A periodic review of policies, procedures, and operational practices maintained by an organization to ensure that they are followed and effective.
Self-Insurance	The pre-planned assumption of risk in which a decision is made to bear loses that could result from a Business Continuity event rather than purchasing insurance to cover those potential losses.
Service Continuity	The process and procedures required to maintain or recover critical services such as "remote access" or "end-user support" during a business interruption.
Service Continuity Planning	A process used to mitigate, develop, and document procedures that enable an organization to recover critical services after a business interruption.

Term	Definition
Service Level Agreement (SLA)	A formal agreement between a service provider (whether internal or external) and their client (whether internal or external), which covers the nature, quality, availability, scope and response of the service provider. The SLA should cover day-to-day situations and disaster situations, as the need for the service may vary in a disaster.
Service Level Management (SLM)	The process of defining, agreeing, documenting and managing the levels of any type of services provided by service providers whether internal or external that are required and cost justified.
Simulation Exercise	One method of exercising teams in which participants perform some or all of the actions they would take in the event of plan activation. Simulation exercises, which may involve one or more teams, are performed under conditions that at least partially simulate 'disaster mode'. They may or may not be performed at the designated alternate location, and typically use only a partial recovery configuration.
Single Point of Failure (SPOF)	A unique pathway or source of a service, activity, and/or process. Typically, there is no alternative and a loss of that element could lead to a failure of a critical function.
Stand Down	Formal notification that the response to a Business Continuity event is no longer required or has been concluded.
Standalone Test	A test conducted on a specific component of a plan in isolation from other components to validate component functionality, typically under simulated operating conditions.
Structured Walkthrough	Types of exercise in which team members physically implement the business continuity plans and verbally review each step to assess its effectiveness, identify enhancements, constraints and deficiencies.
Subscription	See: Recovery Services Agreement / Contract
Supply Chain	All suppliers, manufacturing facilities, distribution centres, warehouses, customers, raw materials, work-in-process inventory, finished goods, and all related information and resources involved in meeting customer and organizational requirements.
System	Set of related technology components that work together to support a business process or provide a service.
System Recovery	The procedures for rebuilding a computer system and network to the condition where it is ready to accept data and applications, and facilitate network communications.
System Restore	The procedures necessary to return a system to an operable state using all available data including data captured by alternate means during the outage. System restore depends upon having a live, recovered system available.
Table Top Exercise	One method of exercising plans in which participants review and discuss the actions they would take without actually performing the actions. Representatives of a single team, or multiple teams, may participate in the exercise typically under the guidance of exercise facilitators.
Task List	Defined mandatory and discretionary tasks allocated to teams and/or individual roles within a Business Continuity Plan

Term	Definition
Technical Recovery Team Test	A group responsible for: relocation and recovery of technology systems, data, applications and/or supporting infrastructure components at an alternate site following a technology disruption; and subsequent resumption and restoration of those operations at an appropriate site. A pass/fail evaluation of infrastructure (example-computers, cabling, devices, hardware) and\or physical plant infrastructure (example-building systems, generators, utilities) to demonstrate the anticipated operation of the components and system. Tests are often performed as part of normal operations and maintenance. Tests are often included within exercises.
Test	An activity that is performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Types of tests include: Desk Check, Peer Review, Structured Walkthrough, Standalone Test, Integrated Test, and Operational Test. Editor's Note: The types of test listed are not exhaustive and the names given tend to vary from country to country. The examples above are those most typically used in North America. Unlike a rehearsal, a test can be a pass/fail evaluation of infrastructure (computers, cabling, devices, hardware) or physical plant infrastructure (building systems, generators, utilities) to demonstrate the anticipated operation of the components and system. A test of this nature will demonstrate whether these parts of the Business Continuity Plan are fit for purpose.
Threat	A potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization, the environment, or the community. Some threats such as bad weather are more commonly referred to as "Hazards".
Uninterruptible Power Supply (UPS)	A backup electrical power supply that provides continuous power to critical equipment in the event that commercial power is lost. The UPS (usually a bank of batteries) offers short-term protection against power surges and outages. The UPS usually only allows enough time for vital systems to be correctly powered down.
Validation Script	A set of procedures within the Business Continuity Plan to validate the proper function of a system or process before returning it to production operation.
Virtual Battle Box	An electronic form of a storage location held on the internet, intranet or cloud so that data and information is immediately available post incident and accessible by the Incident Management Team.
Virtual Command Centre	A means of operating when it is physically impossible for members of the Incident Management Team to move to a Command Centre. A virtual command centre working using telephony and internet solutions including a Virtual Battle Box can be established.
Vital Records	Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the legal and financial

Term	Definition
	rights of that organization and of the individuals directly affected by its activities.
Walk-through	A walk-through is a process whereby BC team members carry out the sequence of the recovery tasks defined in the BC plan. It is also called a Desktop or Table top Exercise. Editor's Note: The objectives of a walkthrough test are to assess the viability of the plan, find flaws and omissions and improve the plan. It also educates management and recovery team members about the plan strategies, limitations and assumptions
Warm Site	An alternate processing site which is equipped with some hardware, and communications interfaces, electrical and environmental conditioning which is only capable of providing backup after additional provisioning, software or customization is performed.
Work Area Facility	A pre-designated space provided with desks, telephones, PCs, etc. ready for occupation by business recovery teams at short notice. May be internally or externally provided.
Work Area Recovery	The component of recovery and continuity that deals specifically with the relocation of a key function or department in the event of a disaster, including personnel, essential records, equipment supplies, work space, communication facilities, work station computer processing capability, fax, copy machines, mail services, etc. Office recovery environment complete with necessary office infrastructure (desk, telephone, workstation, hardware, communications).
Work Area Recovery Planning	The business continuity planning process of identifying the needs and preparing procedures and personnel for use at the work area facility.
Workaround Procedures	Alternative procedures that may be used by a functional unit(s) to enable it to continue to perform its critical functions during temporary unavailability of specific application systems, electronic or hard copy data, voice or data communication systems, specialized equipment, office facilities, personnel, or external services.

APPENDIX B – LIST OF ICT MISSION CRITICAL SYSTEMS

System	Description	Location
CASH DRAWER	Cashier System	**Host Location:**

		Head Office Data Centre, 319 Stateway, Welkom **Backup Routine:** • Daily (Stored On-site) • Weekly (Stored On-site) • Monthly (Stored On-site) **Backup Storage** • No off-site storage. **Proposed Database Replication Site:** **Disaster Recovery Site** Main Building, 6 Union Street, Virginia.
SYNTELL	Prepaid Electricity Vending System	**Host Location:** Head Office Data Centre, 319 Stateway, Welkom **Backup Routine:** • Daily (Stored On-site) • Weekly (Stored On-site) • Monthly (Stored On-site) **Backup Storage** • No off-site storage.

		Proposed Database Replication Site: **Disaster Recovery Site** Main Building, 6 Union Street, Virginia
SOLAR	Financial System	**Host Location:** Head Office Data Centre, 319 Stateway, Welkom **Backup Routine:** • Daily (Stored On-site) • Weekly (Stored On-site) • Monthly (Stored On-site) **Backup Storage** • No off-site storage. **Proposed Database Replication Site:** **Disaster Recovery Site** Main Building, 6 Union Street, Virginia
PAYDAY	HR and Payroll System	**Host Location:** Head Office Data Centre, 319 Stateway, Welkom **Backup Routine:** • Daily (Stored On-site) • Weekly (Stored On-site)

		• Monthly (Stored On-site) **Backup Storage** • No off-site storage. **Proposed Database Replication Site:** **Disaster Recovery Site** Main Building, 6 Union Street, Virginia
PAPERLESS AGENDA	Document Management	**Host Location:** ??????

APPENDIX B1 – LIST OF ICT ESSENTIAL SERVICES

The services listed below and provided by ICT are classified as essential but not critical for Matjhabeng Local Municipality's daily operations:

System	Description
MS Office 365	Matjhabeng Local Municipality has implemented a cloud-based suite of Microsoft applications including OneDrive (personal and shared folders); The key services offered are: • E-mail exchange accounts • Active Directory • OneDrive Redundancy plan guaranteed by Microsoft on availability is 99%.
Internet and Intranet Access	Access to the internet is essential for the users to be able to carry out their daily functions. Without internet access the users will not be able to access the critical services. Matjhabeng Local Municipality's has contracted a service provider to provide a 200 MB line for the Head Office with no redundancy.
Computer Equipment	Matjhabeng Local Municipality's employees have been issued with either a desktop or laptop, and a telephone device. In addition, some IT personnel have been allocated with Laptops. Only 3 do have Desktops Matjhabeng Local Municipality's provides cell phone contracts to some employees. In turn, such employees are required to have their cell phones available for business use at all times.

APPENDIX C – DR PLAN ACTIVATION PROCEDURES

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.
- Initial Meeting of less than 5 minutes is conducted and DRP Champion Informs team to investigate if incident merits declaring a Disaster and asks team to reconvene in 15 minutes with initial assessment and recommendation.
- All affected Business Owners are notified by the DRP Communications Team that there is an outage and they would be given an update in 15 minutes after initial investigations.
- The DR Champion continues mobilising DR Team to ensure the information is ready and available before a Disaster is declared. (Declaring a disaster is expensive and due care and judgement based on objective information is required)

The following template will be used to document the details of interruption. This Template must be completed by the Damage Assessment Team Leader under the guidance of the Acting IT Manager supported by the IT Security & Infrastructure Analyst.

- 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.

- After reconvening the meeting, assessing the extent of the interruption, the Matjhabeng Local Municipality DR Champion takes the decision to Declare a Disaster

1. Incident Description			
Investigation Undertaken			
2. Findings			
3. Recommendations and Action Plan			
Recommendation	Action	By Whom	Due Date
COMMENT			

and from that moment, Actions detailed in DR Test Plan are undertaken

APPENDIX D – DIRECTORY OF DRP CONTACT NUMBERS

CONTACT LIST OF EMERGENCY SERVICES

Fire Department	057 352 2222/4444/1840
Ambulance	082 909 0382/082 522 6526
SAPS	10111/057 391 6000
Disaster Management Centre -	057 352 3317

MATJHABENG MUNICIPALITY KEY PERSONNEL

NAMES	Cell number	Role	Action required
Thabiso Tsoaeli	079 690 0476	Municipal manager	Declare the execution of a disaster recovery plan/ or business continued plan
Puleng Sefuthi	083 586 6200	Risk Officer	Manage the execution of the Business continuity plan
Thembi Xaba	082 717 0369	Procurement	Facilitates procurement of ICT services
Sam Mokhuoa	082 836 6579	Security	Manage Security and Access to the Buildings
Tsholo Mokoena / Ntombi Ntsonta		Facilities Manager	Facilities and Health and Safety Manager
Sipho Nhlapo / Wimpie Jansen	072 991 8860 /	Application representatives	Pay Day sign off post activation of the DRP
Pulane Rakotsoane	082 882 2443	ICT Manager	Manage and Execute the ICT Continuity Plan
Theuns Venter	079 697 0303	ICT Support	Execute the ICT Continuity Plan

TELKOM IT: SERVICE MANAGEMENT

Department		Email address:	Contact numbers:
Service Desk	**Escalation 1**	**Escalation 2**	**Escalation 3**
08 09 339 339	~~Service Manager~~	~~Senior Manager~~	~~Executive~~
	Francois Bartlett	Linton Lazarus	Magda Bester
	012 680 3438	012 648 0031	012 648 0014
	082 770 8857	081 361 5052	

BCX: SERVICE MANAGEMENT

Department	Email address:	Contact numbers:
Service Desk - BCX	Lara <laramail@bcx.co.za>	086 123 9332

Service Desk	Escalation 1	Escalation 2	Escalation 3	
	Manager Service Desk	Account Executive Manager	Senior Manager Expenditure	Senior Manager Income
	Sandra Burger	Chuma Nogemane	Andries Fourie	Potso Mohajane
	012 427 0664	083 581 1513	082 337 2454	083 432 7229

PAYDAY: SERVICE MANAGEMENT

Department	Email address:	Contact numbers:
		086 502 7007

Service Desk	Escalation 1	Escalation 2	Escalation 3	
	Payday Support Manager	Local Government: Customer Care & Sales Manager	Technical Support Manager	
	Jan Engelbrecht (jan@payday.co.za)	MagdaBritz (magda@payday.co.za)	AldoTaylor (aldo@payday.co.za)	
	012-8037730	012-8037730	012-8037730	

CASHDRAWER: SERVICE MANAGEMENT

Department	Email address:	Contact numbers:
Service Desk - BCX	Lara <laramail@bcx.co.za>	086 123 9332

Service Desk	Escalation 1	Escalation 2	Escalation 3	
	Senior Business Consultant	Consultant Business		
	Gideon Joubert (Gideon.joubert@bcx.co.za)	Elna Leimecke (elna.leimecke@bcx.co.za)		
	082 904 2818	012-427 0574		

SYNTELL VENDING: SERVICE MANAGEMENT

Department	Email address:	Contact numbers:
Support		087 267 8779

Service Desk	Escalation 1	Escalation 2	Escalation 3	
	Vending Support Technician	Database Administrator		
	Zukisa Ntsomi (zukisa@syntell.co.za)	Johann v Wyk (johann@syntell.co.za)		
	021 -204 6303	021 -204 6301		

Appendix E: Matjhabeng Local Municipality Incident Report template

Report Prepared by:

{***INSERT YOUR NAME HERE***}

Report Date: {***INSERT DATE***}

1. Incident Description			
Investigation Undertaken			
2. Findings			
3. Recommendations and Action Plan			
Recommendation	Action	By Whom	Due Date
COMMENT			

APPENDIX F – DISASTER RECOVERY SUPPORT TEAMS

Disaster Recovery Champion

Names	Cell number	Role	Action required
Pulane Rakotsoane	082 882 2443	ICT Manager	Declare the execution of a disaster recovery plan/ or business continuity plan

Management Team

Thabiso Tsoaeli	079 690 0476	Municipal Manager	Delegates authority to declare the execution of a disaster recovery plan/ or business continuity plan
			Procurement of ICT services
Sam Mokhuoa	082 836 6579	Security	Access Control
Tsholo Mokoena / Ntombi Ntsonta			Facilities and Health and Safety Manager
Pulane Rakotsoane	082 882 2443	ICT Manager	Manage and execute the ICT Continuity Plan

Damage Assessment Team

The Damage Assessment Team is a technical group responsible for assessing damage to the System and its components. This team is primarily responsible for initial damage assessment, accounting of damage assessment, loss minimization, salvage and procurement of necessary replacement equipment and interfaces.

Names	Cell number	Role	Action required
Pulane Rakotsoane	082 882 2443	ICT Manager	Execute the ICT Continuity Plan
Tsholo Mokoena / Ntombi Ntsonta		Facilities Manager	Assess Facilities Accessibility , Health and Safety Manager

Sam Mokhuoa	082 836 6579	Security	

Server & LAN Recovery Team (e.g., client server, Web server)

Names	Cell number	Role	Action required
Pulane Rakotsoane	082 882 2443	ICT Manager	Execute the ICT Continuity Plan
Theuns Venter	079 697 0303	ICT Support	Execute the ICT Continuity Plan
Tsietsi Vinger	071 643 5674	ICT support	Execute the ICT Continuity Plan
		Desktop Support	ICT Technicians
		Desktop Support	ICT Technicians

Database & Applications Recovery Team

Names	Cell number	Role	Action required
Pulane Rakotsoane	082 882 2443	ICT Manager	Execute the ICT Continuity Plan
		ICT Support	Execute the ICT Continuity Plan
Jan Engelbrecht	086 502 7007	Payroll Representative	Test PayDay and sign off post activation of the DRP
Chuma Nogemane	083 581 1513	Solar representative	Test Solar and sign off post activation of the DRP
Johann v Wyk	083 267 8779	Syntell Representative	Test Syntell and sign off post activation of the DRP

Security Team (IT & Physical)

Names	Cell number	Role	Action required
Jacob Suping	082 836 6579	Security	Declare the execution of a disaster recovery plan/ or business continuity plan
Pulane Rakotsoane	082 882 2443	ICT Manager	Execute the ICT Continuity Plan
		ICT Support	Execute the ICT Continuity Plan

Telecommunications & WAN Recovery Team

Names	Cell number	Role	Action required
Pulane Rakotsoane	082 882 2443	ICT Manager	Execute the ICT Continuity Plan
		ICT Support	Execute the ICT Continuity Plan

Liquid Telecoms	011 585 0094	Liquid Telecoms IT: Service Management	Internet Link
Telkom		Telkom IT: Service Management	MPLS (Multi-Protocol Labelling Services), VOIP/Telephony, WAN (Metro Ethernet)

Alternate Site Recovery Coordination Team

Names	Cell number	Role	Action required
Tsholo Mokoena / Ntombi Ntsonta		Facilities Manager	Facilities Access, Health and Safety
Pulane Rakotsoane	082 882 2443	ICT Manager	Execute the ICT Continuity Plan
		ICT Support	Execute the ICT Continuity Plan

Original Site Restoration/Salvage Coordination Team

Names	Cell number	Role	Action required
Tsholo Mokoena / Ntombi Ntsonta		Facilities Manager	Facilities Access, Health and Safety
Pulane Rakotsoane	082 882 2443	ICT Manager	Execute the ICT Continuity Plan
		ICT Support	Execute the ICT Continuity Plan

Test Team

Names	Cell number	Role	Action required
Tsholo Mokoena / Ntombi Ntsonta		Facilities Manager	Facilities Access, Health and Safety
Pulane Rakotsoane	082 882 2443	ICT Manager	Execute the ICT Continuity Plan
		ICT Support	Execute the ICT Continuity Plan

Communications & Administrative Support Team

Names	Cell number	Role	Action required
		Office Admin – Records Manager	Maintain Records
Pulane Rakotsoane	082 882 2443	ICT Manager	Execute the ICT Continuity Plan
		Communications	Distribute Communications from DRP Champion

Procurement Team (equipment and supplies)

Names	Cell number	Role	Action required
Pulane Rakotsoane	082 882 2443	ICT Manager	Manage and execute the ICT Continuity Plan
Thabo Panyani		CFO	Facilitates procurement of ICT services
Thembi Xaba		Procurement Manager	Facilitating procuring process of required equipment and supplies
Tsholo Mokoena / Ntombi Ntsonta		Facilities Manager	Facilities and Health and Safety Manager

APPENDIX G – DR DAMAGE ASSESSMENT PROCEDURES

Upon receiving information regarding an interruption with the potential for the activation of a Disaster Recovery Plan, the Matjhabeng Local Municipality DR Champion instructs the Damage Assessment Team to begin the process of assessing the damage.

The team will collect and record, using ***Appendix E***, the Matjhabeng Local Municipality Incident Report template, the following in

- 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 C***
- 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.

.

The Damage Assessment Team Leader is to notify his team members and direct them to complete the form below which is also available as ***Appendix E***.

1. Incident Description			
Investigation Undertaken			
2. Findings			
3. Recommendations and Action Plan			
Recommendation	Action	By Whom	Due Date
COMMENT			

APPENDIX H – RECOVERY SITE OPERATION PROCEDURES

This Appendix needs information that is specific to the Recovery Site. We did not have the opportunity to visit the Disaster Recovery Site as the Virginia site is not yet set up/prepared as a DR site. In documenting the Recovery Site Operation Procedures, the procedures assigned to the appropriate recovery team members 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

CASH DRAWER DISASTER RECOVERY GUIDE

MARCH 2019

Last Updated 28 March 2019

Table of Contents

Introduction

This document describes the procedure for disaster recovery for CASHDRAWER in the event of a system failure. This system holds all the account information that is weekly updated from the Financial system.

Background

The Server Specifications for the CASHDRAWER installation are:

Server Name: **MLMC1**

Hardware Specifications
4096 Mb Mem
Hyper-V
2.40GHz CPU
64Bit
126Gb HDD
Software Specifications
Windows Server 2008 R2 Ent 64-bit
SQL 2005;
C/drawer,
Visual Studio

Settings and Checklist

IP Addresses

- The IP Address for Production is: 192.168.1.5
- The IP Address for Backup server is: 192.168.1.8

Port Numbers

Server and Database

- Server Logon is using the Admin user.
- The MSSQL Server Logon is using the Admin user.
- The SQL Server Agent is logging on using the Admin user.

Change configuration checklist

- ✓ IP Address - 192.168.1.5

Connectivity

- ✓ Client to server.

Steps in switching to the backup

This will make the application available for use:

- Ensure connectivity by logging on to Cashdrawer application.
- Install backup exec client on the server.
- Add the server to the backup exec software on the backup server and ensure a trust relationship.
    - Setup client server to perform daily/weekly and monthly backups.
    - Restore data to the server from tape.
- Check that the services are running and logon to the application to see if it's running.

To revert back to the Production Machine / VM

- Do a backup of the database on the Backup Machine that was running as the Production.
- Restore it onto the Production Machine.
- From the Production Machine follow the procedures for Database restore.
- Revert to the original IP address.
- Check connectivity and that the services are running.

PAPERLESS AGENDA DISASTER RECOVERY GUIDE

MARCH 2019

Last Updated 28 March 2019

Table of Contents

Introduction

This document describes the procedure for disaster recovery for PAPERLESS AGENDA in the event that the system goes down. This system is used for document Management for the Matjhabeng Municipality.

Background

The Server Specifications for the PAPERLESS AGENDA installation are:

Server Name:

Hardware Specifications
Software Specifications

Settings and Checklist

IP Addresses

- The IP Address for Production is: 192.168.1.5
- The IP Address for Backup is: 192.168.1.8

Port Numbers

- PAPERLESS AGENDA server is setup with port 80.
- Port 443 is being used for SSL.

- Both ports are enabled in the Firewall.

Server and Database

- Server Logon is using the Admin user.
- The MSSQL Server Logon is using the Admin user.
- The SQL Server Agent is logging on using the Admin user.

Change configuration checklist

✓ IP Address - 192.168.1.5

Connectivity

✓ Client to server.

Steps in switching to the backup

This will make the application available for use:

- Change the IP address of the Backup Server to the Live Server.
- Ensure connectivity by logging on to Paperless Agenda application.
- Add a backup client on the server.
- Add the server to the backup software and ensure a trust relationship.
    - Setup client server to perform daily/weekly and monthly backups.
    - Restore data to the server from tape.
- Check that the services are running and logon to the application to see if it's running.

To revert back to the Production Machine / VM

- Do a backup of the database on the Backup Machine/VM that was running as the Production.
- Restore it onto the Production Machine/VM.
- From the Production Machine/VM follow the procedures for Database restore.
- Revert to the original IP address.
- Check connectivity and that the services are running.

PAY DAY DISASTER RECOVERY GUIDE

MARCH 2019

Last Updated 28 March 2019

Table of Contents

Introduction

This document describes the procedure for disaster recovery for PAYDAY in the event that the system goes down. This system holds HR and Payroll information.

Background

The Server Specifications for the PAYDAY installation are:

Server Name: **PAYDAY**

Hardware Specifications
2000Mb Mem
Hyper-V
2.40 MHz CPU
64bit
126Gb HDD
Software Specifications
Windows Server 2012 R2 Std 64-bit
Payday

Settings and Checklist

IP Addresses

- The IP Address for Production is: 192.168.1.25
- The IP Address for Backup server is: 192.168.1.8

Port Numbers

Server and Database

- Server Logon is using the Admin user.
- The MSSQL Server Logon is using the Admin user.

- The SQL Server Agent is logging on using the Admin user.

Change configuration checklist

✓ IP Address - 192.168.1.25

Connectivity

✓ Client to server.

Steps in switching to the backup

This will make the application available for use:

- Ensure connectivity by logging on to PAYDAY application.
- Install backup exec client on the server.
- Add the server to the backup exec software on the backup server and ensure a trust relationship.
    - Setup client server to perform daily/weekly and monthly backups.
    - Restore data to the server from tape.
- Check that the services are running and logon to the application to see if it's running.

To revert back to the Production Machine / VM

- Do a backup of the database on the Backup Machine/VM that was running as the Production.
- Restore it onto the Production Machine/VM.
- From the Production Machine/VM follow the procedures for Database restore.
- Revert to the original IP address.
- Check connectivity and that the services are running.

SOLAR SYSTEM DISASTER RECOVERY GUIDE

MARCH 2019

Last Updated 28 March 2019

Table of Contents

Introduction

This document describes the procedure for disaster recovery for SOLAR SYSTEM in the event that the system goes down. This system holds all the information about the employees, their employment contract and benefits, leave days and other related salary data.

Background

The Server Specifications for the SOLAR SYSTEM installation are:

Hardware Requirements
Pentium 4 – 2.4 GHz Dual Core Equivalent
2 GB RAM
Available Hard Drive Space
CD/DVD Writer
USB 2.0 Port
Screen Resolution (1024x768) Minimum
100 Mbps Network Card
Software Requirements
Windows Server 2003 with SP2 (32 bit or 64 bit)
Windows Server 2008 (32 bit or 64 bit)
.NET 2.0 Framework

The software installed is listed as:

- Java Development Kit
- Apache Tomcat
- Solar System version 99.99

Settings and Checklist

IP Addresses

- The IP Address for Production is:
- The IP Address for Backup is:

Port Numbers

- SOLAR SYSTEM server is setup with port 80. Port 8080 will be used on test platforms only.
- Port 443 is being used for SSL
- Both ports are enabled in the Firewall

Database

- The MSSQLServer Logon is using the Administrator user
- The SQL Server Agent is logging on using the Administrator user
- The mirroring is using Administrator user

Change configuration checklist

- ✓ IP Address
- ✓ Ports
- ✓ Email addresses
- ✓ Support
- ✓ Reporting
- ✓ Helpdesk

Connectivity

- ✓ Replication
- ✓ Email
- ✓ Switch Database
- ✓ HelpDesk

Steps in switching to the backup

- Stop the mirroring process

  In SQL Query run the 2 SQL Statements below:

  ALTER DATABASE Solar System SET PARTNER OFF

  RESTORE DATABASE *Solar System* WITH RECOVERY

This will make the Database available for use

- Change the IP address of the Backup Server to the Live Server
- Ensure connectivity by logging on to Solar System
- Check that the Tomcat Service is running and logon to the webpage to see if it's running.
- Check that replication is running

To revert back to the Production Machine / VM

- Do a backup of the database on the Backup Machine/VM that was running as the Production
- Restore it onto the Production Machine/VM
- From the Production Machine/VM follow the procedures for Database Mirroring
- Revert to the original IP addresses
- Check connectivity and that the services are running

SOLAR DISASTER RECOVERY GUIDE

MARCH 2019

Table of Contents

Introduction

This document describes the procedure for disaster recovery for SolarApp in the event that the system goes down. This system holds all the Financial Information of the Matjhabeng Municipality.

Background

The Server Specifications for the SOLARAPP installation are:

Server Name: **SolarApp**

Hardware Specifications
VmWare
262144Mb Ram
1274MHz CPU
64bit
1.69 TB allocated space
Software Specifications
Windows Server 2012 R2 Std 64-bit
Solar Fin system

Settings and Checklist

IP Addresses

- The IP Address for Production is: 192.168.1.19
- The IP Address for Backup is: 192.168.1.10 Veeam.

Port Numbers

- SOLARAPP server is setup with port 8080.

- Port are enabled in the Firewall.

Server and Database

- Server Logon is using the bcxdev user.

Change configuration checklist

✓ IP Address - 192.168.1.19

Connectivity

✓ Client to server.

Steps in switching to the backup

This will make the application available for use:

- Make sure Veeam server is running
- Setup server to perform backups, daily, weekly and Monthly.
- Also check backups in folder of the Db server.

To revert back to the Production Machine / VM

- Do a backup of the database on the Backup Machine/VM that was running as the Production.
- Restore it onto the Production Machine/VM.
- From the Production Machine/VM follow the procedures for Database restore.
- Revert to the original IP address.
- Check connectivity and that the services are running.

SYNTELL DISASTER RECOVERY GUIDE

MARCH 2019

Last Updated 28 March 2019

Table of Contents

Introduction

This document describes the procedure for disaster recovery for SYNTELL in the event that the system goes down. This system holds all Prepaid Electricity Vending Information.

Background

The Server Specifications for the SYNTELL installation are:

Server Name: **HOME-PC**

Hardware Specifications
2.80 CPU
2 Gb Mem
32 bit
454 Gb HDD
Software Specifications
Windows 7 Pro SP1 64-bit
MySQL
S3 pre-paid system
Apache Tomcat

Settings and Checklist

IP Addresses

- The IP Address for Production is: 192.168.1.9
- The IP Address for Backup server is: 192.168.1.8

Port Numbers

- SYNTELL server is setup with port 30566.
- Port are enabled in the Firewall.

Server and Database

- Server Logon is using the Admin user.
- The MySQL Server Logon is using the Admin user.

Change configuration checklist

- ✓ IP Address - 192.168.1.9

Connectivity

- ✓ Client to server.

Steps in switching to the backup

This will make the application available for use:

- Ensure connectivity by logging on to Syntell application.
- Install backup exec client on the server.
- Add the server to the backup exec software on the backup server and ensure a trust relationship.
    - Setup client server to perform daily/weekly and monthly backups.
    - Restore data to the server from tape.

Check that the services are running and logon to the application to see if it's running To revert back to the Production Machine

- Do a backup of the database on the Backup Machine that was running as the Production.
- Restore it onto the Production Machine.
- From the Production Machine follow the procedures for Database restore.
- Revert to the original IP address.
- Check connectivity and that the services are running.