INFORMATION TECHNOLOGY CHANGE MANAGEMENT POLICY FOR RUSTENBURG LOCAL MUNICIPALITY

(Directorate: Corporate Support Services) PM/pm

1. STRATEGIC THRUST

The Rustenburg local municipality has adopted the following strategic objectives:

- Drive Optimal Municipal Institutional Development, Transformation and Capacity Building.

2. PURPOSE OF THE REPORT

To submit the Information Technology Change Management Policy to the committee for consideration.

3. BACKGROUND AND RATIONALE

3.1 The Information Technology Change Management Policy is aimed at controlling changes to IT systems and applications that could potentially result in significant system disruption, data corruption or loss.

3.2 A formalized IT change management process is designed to ensure that changes are authorized and operate as intended, and use of information technology in the municipality improves.

3.3 Below is the legislative framework forming the basis of the IT change Management Policy:

- Public Administration Management Act of 2014.
- Control Objectives for Information Technology (COBIT).
- Information Technology Infrastructure Library (ITIL).
- Municipal Finance Management Act of 2003.
- The Electronic Communications and Transactions (ECT) Act 25 of 2002.
- National Strategic Intelligence Act 2 of 2000 applicable for South Africa.
- Municipal System Act 2000 as amended.
- State Information Technology Act 88 of 1998.

4. LEGAL COMMENTS

4.1 The attached policy has been developed by Directorate Corporate Support Services for purpose of enabling the Municipal Council to approve and adopt this policy. This policy is also applicable to Managers directly accountable to the Municipal Manager. The authority of the Council to approve and adopt these policies in informed by the following legal prescripts: -

4.1.1 Section 4 of the Municipal System Act which *inter alia* provides that the Council of the Municipality has the right to govern on its own initiative in matters of local government affairs.

4.1.2 Section 4(2) of the Municipal System Act *inter alia* provides that the Council should provide without favour or prejudice, democratic and accountable government and promote a safe and healthy environment in the municipality.

4.1.3 Section 11 of the Municipal System Act 32 of 2000 provides that the Municipal Council has the legislative and executive authority to take decisions. The Municipal Council *inter alia* exercises its legislative or executive authority by developing and adopting policies, strategies, establishing and maintaining an administration, administering and regulating its internal affairs, monitoring the impact and effectiveness of any services or policies or programmes or plans, promoting a safe and healthy environment within its legislative and executive competence.

4.1.4 These policy is necessary to enable the municipality to adopt to the ICT volatile environment which is rapidly changing and opening many end users vulnerable to cyber-attacks and outdated systems. Notwithstanding its enabling factor, such changes must be implemented with due considerations of existing contractual and statutory obligations which the municipality may have.

5. FINANCIAL IMPLICATIONS

5.1 Purpose of the report is to request the council to approve the IT Change Management Policy.

5.2 It is recommended that the policy be implemented for internal control purposes.

5.3 In terms of the report the policy is aimed at promoting effective, efficient, and acceptable internal control measures by ensuring that the acquisition, governance, management and use of information technology in the municipality improves.

5.4 Budget and Treasury Office recommends that the Information Technology Change Management Policy be considered.

RECOMMENDATIONS	**ACTION**
1. That the Information Technology Change Management Policy be noted;	PFC
2. That the Information Technology Change Management Policy be recommended to Council for approval	PFC

Rustenburg Local Municipality

IT Change Management Policy

1. Policy Statement

1.1 Rustenburg Local Municipality (“RLM” or the “Municipal”) formally manages changes to its Information Technology (“IT”) resources to prevent disruptions to the stability or integrity of Municipal IT systems, applications and data loss.

2. Background

2.1 Uncontrolled changes to IT systems and applications could potentially result in significant system disruption, data corruption or loss. A formalized IT change management process is designed to ensure that changes are authorized and operate as intended.

3. Policy Objective

3.1 The objective of this policy is to define formal requirements to manage changes to IT systems and applications, in order to prevent unscheduled disruption, data corruption or loss.

4. Scope

4.1 This policy applies to:

4.1.1 All IT systems or applications managed by RLM that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

4.1.2 All change requests to IT systems and applications, including standard, minor, major and emergency changes.

5. Definitions

5.1 **IT Change** is a planned modification to an IT system.

5.2 **Emergency IT Change** is an unplanned modification to an IT system that requires immediate implementation to correct an important issue, such as a disruption or outage of service.

5.3 **Information Technology Steering Committee (IT STECO)** is a committee of senior management that directs, reviews, and approves IT strategic plans, oversees major initiatives, and allocates resources.

Members of the IT STECO include the Director: Corporate Support Services and IT Manager. IT Personnel and system owners. The chairperson of the IT STECO is the Director: Corporate Support Services.

5.4 **Change Approver** is the IT Manager/Director that is responsible for approving a minor change, bringing a major change to the IT STECO for approval, or an emergency change for approval.

5.5 **Change Implementer** is the IT staff member that is responsible for ensuring that the documentation, testing, and implementation of a change is complete.

5.6 **Change Requestor** is the user that initiates the change request.

6 Guiding Principles

6.1 The IT Unit will apply a formal approach to managing IT systems and applications changes.

6.2 Changes to IT systems and applications must be managed in accordance with the IT Change Management Guidelines contained in Appendix 1.

6.3 All change requests must be:

6.3.1 Classified before being processed. The level of analysis, approval and testing must be aligned with the change classification level in order to address potential risks.

6.3.2 Approved prior to commencing the change or development, and prior to implementing the fully tested change into the live environment.

6.3.3 Documented before, during and after implementation. See Appendix 2 for a sample of the type of information required for a Request for Change (“RFC”).

6.4 Business value, business risks, technical risks (including potential impact to performance and security risks), as well as costs must be formally considered before authorizing changes.

7. Roles and Responsibilities

Stakeholder	Responsibilities
Municipal Council	• Approve and formally support this Policy.
Director: Corporate Support Services	• Review and formally support this Policy.
IT Manager	• Develop and implement this Policy. • Take proactive steps to reinforce compliance of all stakeholders with this Policy. • Communicate with the Municipality, directly or through Municipal representatives, in informal or formal instances, to understand the Municipal needs and expectations, explain the capabilities of the existing technology in production, and facilitate the process to manage change requests. • Report to the IT STECO, the Municipal Manager and the Council about the major changes.

8. Exceptions to the Policy

8.1 Exceptions to the guiding principles in this policy must be documented and formally approved by the Director: Corporate Support Services, with evidence of support from IT STECO.

8.2 Policy exceptions must describe:

8.2.1 The nature of the exception.

8.2.2 A reasonable explanation for why the policy exception is required.

8.2.3 Any risks created by the policy exception.

8.2.4 Evidence of approval by the Director: Corporate Support Services.

9. Inquiries

9.1 Inquiries regarding this policy can be directed to the IT Manager.

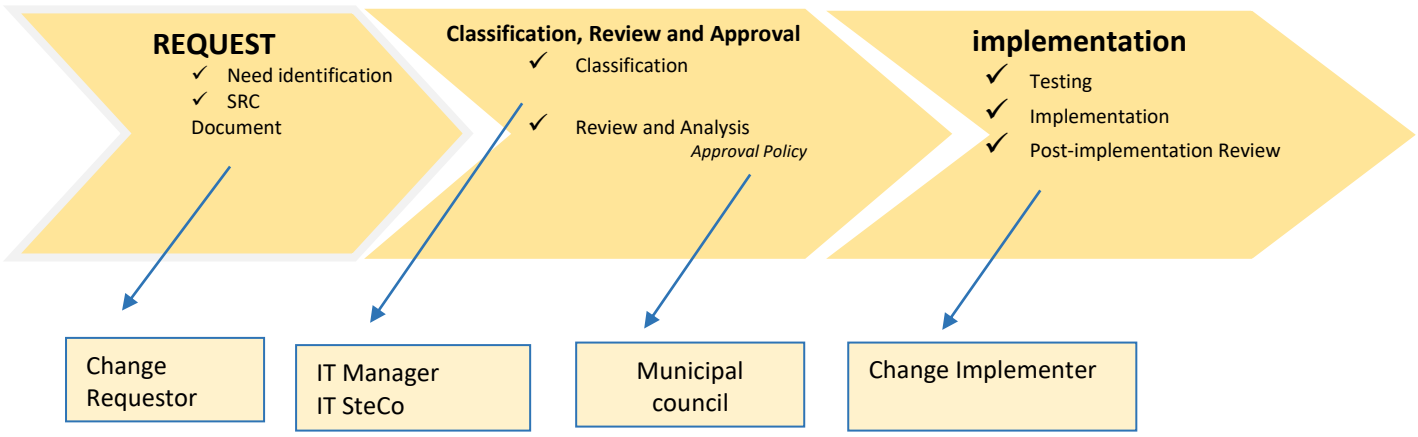
10. Amendments (Revision History)

10.1 Amendments to this policy will be published from time to time and circulated to the Municipal personnel.

APPENDIX 1

APPENDIX 1 – IT Change Management Policy Guidelines

All change requests must be managed according to the principles illustrated in the flowchart diagram:



1 **Request for a change to IT Systems**

1.1. Identification of the need for a formal change request

1.1.1. A new request for change can be initiated by any user.

1.1.2. The need for an IT change can be the result of an IT incident or problem, a new system release, or a specific request, including, for example:

1.1.2.1. Commissioning or decommissioning an IT system or service.
1.1.2.2. Modifying a system configuration that requires IT involvement.
1.1.2.3. Developing, coding, scripting, or programming a system or application.
1.1.2.4. Patching and updating system firmware, operating system or software.
1.1.2.5. Making bulk changes to systems and data in production, outside of standard business operations or application functionality processes.
1.1.2.6. Modifying security group, roles and privileges.
1.1.2.7. Modifying the security configuration of IT systems, applications and networks.

1.1.3 IT change requests must be first processed by the IT Service Desk, a representative from IT or the IT Manager, who will confirm the need to submit a formal request or identify alternative options where appropriate.

APPENDIX 1

1.2. Documentation of changes

1.2.1. The change request must be documented in the request tracking system (Service Desk), and the change management fields must be filled in. The requested change must:

1.2.1.1. Identify the change requestor, change resources, change implementer, and change approvers.

1.2.1.2. Contain sufficient details to facilitate a clear assessment of the risk and demonstrate sufficient planning.

1.2.1.3. Be communicated to the appropriate stakeholders for validation and assessment, and be approved through the tracking system before implementation.

1.2.2. The change implementer is responsible for ensuring that:

1.2.2.1. The initial classification of the change request is accurate.

1.2.2.2. All required documentation is recorded (as per section 2.1).

1.2.2.3. All required approvals are in place (as per section 2.1) before starting or implementing the change.

1.2.2.4. Status updates, such as approval and completion status, are Maintained throughout the life cycle of the change (from creation to completion, or cancellation).

2. Classification, Review and Approval of New Changes Requests

2.1 Change Classification

There are four types of Information Technology changes as follows:

Change Type	Criteria	Supporting Documentation
Emergency Change	• A change that requires immediate implementation to correct an important issue, such as a disruption or outage of service. • Examples of emergency changes include: repairing an IT service issue that severely impacts the business, or a situation that requires immediate action to either restore a service or prevent an outage.	Documentation can be provided after the change has been implemented. • Change request. • IT STECO approval. • Post

Change Type	Criteria	Supporting Documentation

	• An emergency change requires:
	  • Sufficient review and discussion with all impacted and involved parties, including business users, the IT Manager of the team performing the change.
	  • Approval by the IT STECO prior to implementation. At minimum, approval should be from at least one member of the IT STECO and the system owner.
	  • Testing may be reduced, or not performed altogether if necessary, and may be performed after implementation.
	  • Submission of a change request within one business day after the issue has been resolved.
	  • Post-implementation review performed by manager of the team that performed the change and provided to the IT STECO.
		implementation Review.

Major Change	A change that is high risk and complex, with a significant potential impact to production services, and limited backup/recovery in the event of an issue. A major change requires: • Formal review and discussion with all impacted and involved parties, including business users, the IT Manager of the team performing the change. • Formal testing (when possible). • Formal review and approval by the IT STECO prior to implementation.	• Change Request. • Risk assessment. • Implementation plan. • Test plan/results (when possible). • Back-out plan. • IT STECO approval. • Post implementation review.
Minor Change	• A change that is low risk and well understood, with a limited potential impact to production services, is sufficiently tested prior to implementation and is easy to back-out in the event of an issue. • A minor change requires approval to start from the manager of the team performing the change, and approval from the system owner prior to going live or upon completion.	• Change Request • Test plan/results (when possible) • Approvals

Change Type	Criteria	Supporting Documentation
Standard Change	• A change that is low risk and relatively common, where the implementation follows a simple documented procedure or work instruction. For example, password reset or provision of standard equipment to users. • A standard change follows a formal procedure or work instruction that has been authorized in advance.	• Standard Change Procedure Authorization

2.2. Change review and analysis

2.2.1. Business value, business risk, technical risk, and cost must be assessed as part of a formal review of new change requests, by stakeholders from the Institution and IT.

2.2.2. Business value and risk includes the following:

2.2.2.1. Value to Institution operations and alignment with business objectives and requirements.

2.2.2.2. Potential impact and risk to Institution operations if the change is implemented.

2.2.2.3. Potential impact and risk to Institution operations if the change is not implemented.

2.2.2.4. Timing of the change to minimize impact to operations.

2.2.2.5. Acceptance and adaptation by affected parties and users.

2.2.2.6. Potential security risks introduced by the change.

2.2.3. Technical risk includes the following:

2.2.3.1. Complexity of the change.

2.2.3.2. Complexity of the system or infrastructure affected by the change.

2.2.3.3. Interdependencies between different system components and IT services.

2.2.3.4. Impact on normal IT operations, including: system usage, disaster recovery plans, back-up and storage, hardware and software, and change to operational procedures.

2.2.3.5. Technical feasibility of the change and level of effort for IT and the Institution.

2.2.3.6. Availability of resources with required technical expertise.

APPENDIX 1

2.2.4. Cost elements include the following:

2.2.4.1. Costs associated with not implementing the change, such as penalties due to non-compliance or loss following a disruption of the current systems or services. If possible, potential return on investment (ROI) should be estimated.

2.2.4.2. Total Cost of Ownership (TCO), including one-time purchases (software, hardware and professional services) and ongoing maintenance costs.

2.2.4.3. People costs (hourly rate, overtime, travel expenses, etc.)

2.2.4.4. External costs (consulting services, third party outsourced services).

2.2.4.5. Training costs.

2.2.4.6. Communication costs.

2.2.5. Information Technology Unit must ensure that that major changes are communicated to the appropriate stakeholders to review the criteria listed above. This includes, at minimum the:

2.2.5.1. Change Requestor's manager.

2.2.5.2. Impacted IT team.

2.2.5.3. IT Manager or leader of the team that will implement the change.

2.2.5.4. Director: Corporate Support Services or its representative.

2.2.6. The Change Requestor must provide sufficient information to analyse the Change request prior to submitting the change request for approval. When the Change Approver reviews a change request, they either:

2.2.6.1. Approve or deny the proposed change (standard / minor changes).

2.2.6.2. Bring change request forward to the IT STECO (major changes)

2.2.6.3. Convene an urgent IT STECO meeting to review the change request (emergency changes)

2.2.6.4. Request additional information by sending the change request back to the Change Implementer for further investigation and analysis.

2.3. Approval

2.3.1. Major and Emergency change requests must be formally approved by the IT STECO or, Its respectively.

2.3.2. Information Technology Steering Committee shall make decision about Major Changes and meets regularly, as required.

2.3.3. Information Technology Steering Committee shall make decisions about high-impact Emergency Changes and meets upon request by the Director: Corporate Support Services in consultation with the Municipal Manager.

APPENDIX 1

3. Implementation and Status of Change Requests

3.1. Testing

3.1.1. All changes must be tested, when possible, prior to implementation in production.

3.1.2. Tests of changes must be performed in a non-production environment, Where possible.

3.1.3. A test plan must be formally documented, where possible, and approved by IT Unit and Municipal Management:

3.1.3.1. The test plan must identify the specific test scenarios or scripts that are to be executed, what types of testing are required (unit testing, integration testing, user acceptance testing, etc.) and the way in which success or failure will be determined for each test.

3.1.3.2. At a minimum, the test plan must include testing activities to verify that the change has the desired impact and that there has been no adverse impact to service stability. Additional testing may be appropriate for complex or risky changes.

3.1.4. Test results must be documented in the tracking system.

3.2. Implementation

3.2.1. Changes must only be released in production when:

3.2.1.1. Test results are accepted by Municipality and IT Unit.

3.2.1.2. All tests have sufficiently passed. Any failed tests must have a clearly established remediation plan or represent an acceptable level of risk that has been accepted by the Change Approver.

3.3. Post-Implementation Review

3.3.1. A post-implementation review must be performed by stakeholders to confirm the change is complete or to identify remaining issues.

3.3.2. The status of the change must be updated based on the results of the post-implementation review.

3.4. Regular review of Change Request status

3.4.1. The status of incomplete change requests must be regularly reviewed in IT STECO meetings, until the change is either dismissed or fully implemented.

3.4.2. An annual review of open change requests must be performed by the IT Manager to identify and follow-up on old RFCs that have not been closed.

3.5. Policy Review

3.5.1 This policy will be reviewed after two years from date of adoption and may also be reviewed when there is a need to address a critical issue not addressed or not adequately addressed by this policy. The policy may also be reviewed to address issues as indicated by the Auditor General's Office.

4. Roles and Responsibilities

Stakeholder	Responsibilities
Risk Management Committee	Review change requests, including their potential impacts and level of risk. Provide formal approval to implement change requests. Review change progress with respect to the approved schedule, and participate in Post Implementation Reviews. Provide recommendations regarding the implementation of changes into production, prioritize change requests, and make decision if any conflict occurs. Provide recommendations to improve or update this Policy.
Information Technology Steering Committee (IT STECO)	Meet upon the request of the Director: Corporate Support Services Review urgent change requests and: o Confirm the level of urgency; o Evaluate the potential impacts and risks; o Formally authorize the implementation of emergency changes where appropriate; o Ask for additional information where needed; and o Make any other decisions to address issues and concerns.
IT Manager	Review the status of existing change requests. Ensure change requests are: o Following the present Policy; o Fully documented with all necessary details; o Communicated to the appropriate stakeholders (Director and IT Personnel) for comment, before presented to the IT STECO for approval; o Presented to the IT STECO for approval. o Addressed in a timely manner by the Change Implementer after IT STECO approval. Communicate with the Change Requestor and the Business to confirm specific aspects of the requests, as well as scheduling. Participate in the remediation of any problem, issue, incident and conflict resulting from a change by escalating to the right

Stakeholder	Responsibilities
	stakeholder or IT STECO meeting. Provide recommendations regarding the implementation of changes into production, prioritize change requests, and make decision if any conflict occurs. Provide recommendations to improve or update this Policy.
Director: Corporate Support Services	Chair the IT STECO meetings, including presentation of the status of all change requests (new, pending, issues, completed) and formal documentation of IT STECO meeting minutes or decisions. Provide recommendations to improve or update this Policy.
Change Implementer (IT Personnel)	Verify the appropriate classification of the change and evaluation of the risks. Prepare the implementation of the change request, including some elements of analysis, work scheduling, design, build, test, and roll-back / back-out activities. Test changes and report any issue or negative impact. Implement successfully tested and approved changes into production. Update system documentation. Report to the Change Approver on the status of all changes assigned to her/him. Communicate with the Change Approver, the Change Requestor and any related key stakeholders to better understand the request for change, report errors, issues, or delay in testing or implementing the change. Escalate problems and incidents resulting from deploying changes. Participate in post-implementation reviews as required by the Change Approver.
Change Requestor	Initiates a Request for Change (RFC) with the required details. Answer all additional information required by the Change Implementer, the Change Approver, IT stakeholders, or the IT STECO. Communicate with business stakeholders to ensure business requirements are met. Participate in acceptance testing and post implementation reviews as required.
IT Service Desk	Respond to any user requesting an IT Change. Verify the nature of the request and confirm if a formal change request is necessary. Identify the change classification and immediately inform the Change Implementer or Change Approver where necessary. Enter detailed information in the tracking system, including the name of the Change Requestor and description of the

Stakeholder	Responsibilities
	change. Update the status of the change as required.
Supervisors or Municipal representatives	Review any problem, issue or need from users that would require a new change request. Approve new change requests initiated from users. Communicate with the IT personnel to submit a new change request
Users	Contact the IT Service Desk for any questions or concerns related to the technology. When a question or concern cannot be addressed by the Help Desk, contact their supervisor or representative. Contact their supervisor or manager for any request to change the existing technology.

Appendix 2 – Request for Change (RFC) Form

Please complete and send to: IT Help Desk

1 General Information – Section 1	
Requested By	
Change Requester	
Requested Date & Time	
Change Request Number	
Change Implementer	
Change Approver	
System Owner	
Classification	
2 Brief Description of the Change Request	
3 Risk and Impact of not Implementing this Change	
4 Potential Risk and Impact related to the implementation	
Business Risk: **Technical Risk:** **Security Risks:**	
5 Schedule	
Requested Implementation Start Date & Time	

Requested Implementation End Date & Time	
6 Implementation Plan	
7 Test Plan	
8 Back-out Plan	
9 Other/ Comments	