Blouberg Municipality

IT CHANGE MANAGEMENT POLICY

GLOSSARY

1. **"BLM"** refers to Blouberg Local Municipality.
2. **"BLMITO"** — refer to Blouberg Local Municipality Information Technology staff members
3. **"IT"** — refer to Information Technology
4. **"CoBIT"** refers to control Objectives for Information and related Technology
5. **"ICT"** refers to Information Communication Technology
6. **"ITIL"** refers to Information Technology Infrastructure Library
7. **"SIP"** refers to service Improvement plan
8. **"CRP'** refers to Change Request Forms.
9. **"email"** refers to electronic
10. **"CFO"** refers to Chief Finance Office

1.PURPOSE

1.(1) The primary purpose of this policy is to put in place control processes that ensures adherence to this policy when carrying our Municipality duties, by following a set of guidelines when effecting changes to BLM IT Infrastructure.

(2) The Blouberg Local Municipality Information Technology Office (BLMITO) has developed the Information Technology Security Policy that shall apply to all Blouberg Local Municipality officials, its contractors, service providers, interns, students, councillors, and other authorised 3rd party entities that will need the municipality's IT Infrastructure in order to perform their respective duties at BLM.

(3) The purpose of this policy is to protect the municipality's Information Technology resources and to safeguard and control changes to BLM IT Infrastructure.

(4) This policy serves to guide all who are responsible for affecting changes to Information Technology Infrastructure for purposes of investigation, analysing, assessing, testing and implementing changes.

(5) The policy seeks to minimize disruption to Information Technology services at Blouberg Local Municipality (BLM).

2. USER AWARENESS

(1) Every councillor, employee, contractor and authorized 3 rd party entity should become familiar with the policy's provisions and the importance of adhering to it when effecting changes to BLMM IT Infrastructure.
(2) Popularization of this policy will be conducted through presentations to all staff members.
(3) All officials shall attend presentations of this policy and sign on the attendance register as acknowledgement of knowledge of the contents of this policy and repercussions of its transgression.
(4) This policy will be send using email to all users of ICT services and it is expected of all users to familiarize themselves with the contents and provisions of this policy.

4. DOCUMENTS THAT SHOULD BE READ WITH THIS POLICY

(1) Password policy
(2) Security Policy
(3) ICT Equipment policy
(4) Network Access Policy

5. SCOPE

(1) The scope of the policy covers ant IT related equipment or asset and includes and not limited to software, hardware, applications, documents, plans and procedures relevant to running, support and maintenance of Information Technology Systems.

(2) The following is an incomplete list of common reasons why change is needed: (a) User request
(b) Vendor recommended/required changes
(c) Changes in applicable laws
(d) Hardware and/or software upgrade
(e)Acquisition/implementation of new hardware or software
(f) Hardware or software failure
(g) Changes or modifications to the infrastructure
(h) Environmental changes (electrical, air conditioning, data centre remodels, etc)
(i) Change in Technology
(j) Unforeseen events
(k) Periodic Maintenance
(l) Application modifications and enhancements (m) Patch deployment

6. SCOPE OF APPLICATION

(1) This policy shall apply to all employees of Blouberg Local Municipality, councillors, interns, learner ship students, contractors, third party service providers and any other person or system granted permission to use IT Infrastructure of BLM.

7. ROLES AND RESPONSIBILITIES

(1) All BLMITO Team members are responsible to make sure that they are keeping changes in compliance with the Municipality's IT Change Management policy. It is the responsibility of every user of IT Infrastructure to ensure adherence to his Change Management Policy.
(2) BLMITO is responsible for informing users of prospective changes that affects them through email.

8. LEGAL FRAMEWORK

(1) Any employee found to have violated this policy may be subjected to disciplinary action, up to and including termination of employment.

(2) Employees who violate this policy will be disciplined in terms of measures contained in or published in one or more of the following acts, regulations, and policy prescripts (this list is by no means exhaustive):

(3) The constitution of the republic of South Africa

(4) The state Information Technology Act

(5) SITA Amendment Act

(6) Promotion of Access to Information Act

(7) Municipal service Act.

(8) Municipal Finance Management Act

(9) National Archives Act.

(10) Protection of Government Information Act

(11) Telecommunication Act

(12) Telecommunications Amendment Act

(13) Various other statuses

(14) Any other application legislation, regulation or policy of BLM

9. DIRECTIVES AND DEPENDANCIES

(1) All IT changes must adhere to this Blouberg Local Municipality Information Technology Office Change Management Policy. Product, services, and infrastructure changes must have a clearly defined and must have documented scope, with desired outcome .

(2) The policy must be popularized and distributed to all Municipal staff members, councillors and all computer users. It should be also introduced to stakeholders, third party service providers, prospective computer users and all concerned parties.

(3) Directives

(a) All changes will be recorded by BLMITO. Everybody who initiates changes to IT Infrastructure shall follow the directives of this policy to effect such changes.

(b) Such changes shall be recorded, controlled and implemented within the documented IT change management process.

(c) There will be no exception to this directive, unless duly authorized, complete and comprehensive records from the basis of the strategic decisions.

(d) Under no circumstances shall any changes be affected without proper records duly signed.

(e) In the events of a major emergency IT back-end changes shall be classified and managed according to the change management procedure.

(f) For as long as such changes will not have effects on how end users discharge their work.

(g) The policy shall be brought to the attention of all new and existing staff and other relevant stakeholders through presentations at workshops.

(h) All those who attend the presentations and workshops for this policy shall confirm their attendance register on the provided attendance register.

(i) Signing the attendance register confirms understanding the contents of this policy and acknowledging this policy.

(j) All members of BLMITO shall confirm receipt and acknowledge comprehension of this specific policy by signing within seven (7) days of employment or within 30 days of the policy being approved or reviewed.

(4) Dependence

(a) Political commitment
(b) Senior Management Commitment
(c) Commitment and acceptance to change by all staff members
(d) Adherence to change management process and procedure
(e) Competence, awareness and training of all
(D Training of BLMITO Team
(g) Adherence by BLMITO Team

10. CHANGE MANAGEMENT

(1) The role of change management process is to ensure that new services and IT changes to render services are assessed, approved, implemented and reviewed in a controlled manner with minimum risk to the business of BLM.

(a) Change analysis

(i) Change records must be analysed regularly to detect increasing levels of changes, frequently recurring types, emerging trends and others relevant information.

(ii) The results and conclusions from IT change analysis shall be recorded.

(iii) Action for improvement identified from IT change management shall be recorded and input into a service improvement plan (SIP) for improving the service.

(b) Change initiation

(i) All operational IT changes need to be submitted to the IT Manager.

(ii) All change requestors must complete the CRF, and mandatory fields must be completed or the CRF will not be considered for approval.

(c) Change classification

(i) All changes need to be classified according to how much impact they will have on the business and service provision

(ii) Below, are some clear definitions of types of changes, these changes will all have different priorities based on assessed urgency and impact levels depicted further below.

(d) Planned major changes

(i) Changes that result in business interruption during regular business hours.

(ii) Changes that result in business or operational practice change.

(iii) Changes in any system that affects disaster recovery or business continuity

(iv) introduction or discontinuance of a new or existing information technology service.

(e) Maintenance and minor updates

(i) Operating system patches (critical, hotfixes, and service packs).

(ii) Regularly scheduled maintenance.

(iii) Application-based security or business needs patches

(iv) A change that is not likely to cause a service outage.

(v) A change that affects only a single user will be "verbal approved from IT manager".

(f) Emergencies and unplanned outages changes

(i) Building is completely without IT services.

(ii) A severe degradation of service needing immediate action

(iii) System/application/component failure causing a negative impact on municipality operations.

(iv) A response to disaster.

(v) A response to emergency responder personnel.

(vi) (vi) Emergencies and unplanned outages.

11. CHANGE PRIORITIZATION

(1) Change prioritization will be based in two things i.e. Potential impact associated with the service and SLA's affected (impact) and speed with which the change needs to be effected (urgency).

(2) Change prioritization is the sequence in which changes need to be rolled-out or implemented, based on impact and urgency as defined below.

(3) The rationale for this approach is that although the impact associated with a particular change might be high, the urgency to have it might be low, thus enabling IT officials to strategically commit resources and capabilities.

(4) Although it is likely that a high impact change will be urgent, this is not always the case.

(a) Priority

(i) Priority must be associated with the service affected or potentially affected.

(ii) Changes must be identified to allow correct classification according to potential impact of the service.

(iii) The quickly and accurately establishes the changes urgency and its impact on the business.

(iv) It also records the expected timescale for return to normal and specified the arrangements for the invocation of business continuity planning.

(b) Impact

(i) This signifies business impact and criticality.

(ii) The impact of a change must be determined by the effect it has on the business and the customer.

(iii) Factors that must be considered are:

(iv) The number of customers/users affected or could potentially be affected, the extent to which business degradation results and the stage in the business cycle when the change is implemented.

i. Severe- Any change where the impact could lead to loss of service or could potentially pose a threat to the integrity of the whole municipality.

ii. Major- A change where the potential impact to service could lead to a loss of more than 50% of total capacity or loss of more than 50% of set targets (origins/destinations) not reachable.

iii. Significant — A change where the potential impact could lead to a loss less than 50% of total capacity or loss of all redundancy (exposure to complete service outage) or a loss of a set target (origin/destination not reachable)

iv. Minor — A change where the potential impact could degrade the quality of service or affect a small number of users e.g., a

change to a printer used by the user in the department (risk is less).

v. Inconsequential - Any change that doesn't have any potential to impact directly on service delivery in respect of existing service to existing customers such as: request for a new service, amendment of supporting documentation or a change with a set release mechanism (standard change)

(c) Urgency

(i) Critical — immediate action required. Changes, if not implemented immediately will leave the department open a huge risk (financial and/or other). All severe impact changes will have a critical urgency but not all critical urgency changes would have a severe impact.

(ii) High — A change that must be implemented but doesn't have a severe impact.

(iii) Medium — A change that must be implemented as soon as possible, associated with partial denial of service with an impact on a large number of customers.

(iv) Low — A change that must be implemented as soon as possible, associated with the partial denial of service on a limited number of customer or degradation in the quality of service.

(v) Schedule — A change that is not required to be implemented as classified above or request for a new service

12. ROLL BACK PLANNING

(1) The IT change management process should include the manner in which the change is to be reversed or remedied if unsuccessful

(2) All changes must be approved and implemented in a controlled manner and according to the documented process.

(3) All changes shall be reviewed for success and any action taken after implementation. (4) A forward schedule of changes that contain details of all the changes approved for the implementation and their proposed implementation dates shall be maintained and communicated to relevant parties.

13. CHANGE APPROVAL

(1) All changes shall be approved by the Manager IT.

(2) The IT manager shall at all material times advise the municipality on all the technical changes through written email or any other form of communication.

14. CHANGE AUTHORIZATION

(1) Change prioritization

(a) All changes must be reviewed after implementation and the results of this reviewed must be documented. This review must be covered by then following:
(b) Weather the change met its objectives, if not the reasons must be documented, and improved actions identified.
(c) Weather the change has an impact on the customer's business operations.
(d) Weather the implementation went as planned and if not, weather the back out plan worked.

(2) Change freeze period

(a) Change freeze periods are imposed in order to protect the municipality IT infrastructure, applications and/or other business operations from any change that may undermine its stability and operations.
(b) The change freeze periods depend largely on what information you have from the business, ideally BLMITO should have a calendar of business events well ahead of schedule where you could identify times and dates when change freeze required, this way everyone knows well in advance that they will not be able to make changes at that and can therefore plan around them.
(c) Annually a change freeze will be observed when going through the financial year end process, in which the entire municipality is affected
(d) This period shall be negotiated with the CFO of the municipality and any changes during this period can only be approved by CFO.
(e) The agree timeline shall be communicated to all, three months before time to allow adequate planning and pre-freeze implementation.

15. NON-COMPLIANCE

(I) Where non-compliance by officials is found, necessary disciplinary steps will be taken to remedy the situation.
(2) The remedy may include actions per the municipality's disciplinary code of conduct and could lead to dismissal.

16.POLICY APPROVAL

This policy was formulated by IT Division in consultation with the Local Labour Forum.

Authorised by Municipal Manager: Signature: _____ **Date:** 30/07/2024

Recommended by Portfolio Committee on Corporate Services: Signature: _____ **Date:** 30/07/2024

Approved by Municipal Council: Signature: _____ **Date:** 30/07/2024