FETAKGOMO TUBATSE
LOCAL MUNICIPALITY

CHANGE CONTROL POLICY AND PROCEDURES

Council Resolution NR: OC148/2018

Version Control

Version	Date	Author(s)	Details
Ver. 1.0	10/07/2017		Change Management Policy

Approvals

DESIGNATION	NAME	SIGNATURE	DATE
Director: Cooperate Service			
Municipal Manager			
Mayor			

TABLE OF CONTENTS

CHAPTER 5

PLANNED MAINTENANCE

CHAPTER 6

EMERGENCY MAINTENANCE

CHAPTER 7

CHANGE OF ACCESS RIGHTS TO DOMAIN AND/OR SYSTEMS

CHAPTER 8

PROCEDURE APPROVAL AND VERSION CONTROL

CHAPTER 1

INTERPRETATION, PURPOSE AND APPLICATION OF THE PROCEDURES

1.1 Definitions

1.1.1 **Application:** A system that provides a specific set of functions and/or services to end users. It usually refers to a common software application like Accounting Software i.e. E-Venus.

1.1.2 **Application Owner:** The business owner of an application utilized within Fetakgomo - Greater Tubatse Municipality.

1.1.3 **Life Cycle:** The life of a system measured from inception through retirement. A typical life cycle will have the following mile stones: requirements analysis; design, build, test, roll-out, sustainment and retirement. Each milestone may be interactive because systems usually undergo continues refinement. As such a system at the sustainment milestone will have many interactions of requirements-design-build-test-implement as it is upgraded to add new functions and features and fix defects.

1.1.4 **Maintenance Window:** Time set aside to perform normal system maintenance, such as back-ups, preventative mechanical maintenance, upgrades, etc. Maintenance windows are defined in Service Level Agreements (SLA) as a function of availability. For example: A service level objective for a business-critical system might state that the system will be available on a 24/7 basis for twenty consecutive days, with a four-hour period set aside every 21st day to perform maintenance. This four hour period is the maintenance window.

1.1.5 **Municipality:** Fetakgomo - Greater Tubatse Municipality

1.1.6 **Planned Maintenance**

(1) Recurring maintenance such as back-ups that are scheduled to take place during a specific maintenance window.

(2) Maintenance requirements, such as upgrades and patches, that are scheduled in accordance with an implementation plan to occur during a maintenance window.

1.1.7 **Pre-Production Environment:** A test environment that is configured identically to the production system. The purpose of this environment is to test patches and minor releases for defects prior to implementing them into the production environment. A secondary purpose, when applicable, is to verify and validate functions and features that were included in a minor release or patch.

1.1.8 **Roll-back:** To uninstall or remove a change and restore a system to it's previous state.

1.1.9 **Roll-out:** Milestone in the system development life-cycle that occurs after successful completion of user acceptance and quality control testing but prior to post-implementation verification.

1.1.10 **Service Level Objective (SLO):** An objective or goal in support of providing services i.e. availability, key transaction performance, uptime, etc. Service Level Objectives are the foundation of Service Level Agreements.

1.1.11 **System:** A collection of subsystems and components that comprises an integrated environment that provides services or functions. Systems are typically comprised of hardware and software, and many include databases, middleware and communications facilities.

1.1.12 **Technical Domain:** A functional area defined by related technical specialities. For example, database management is technical domain that includes data architects, database administrators, and data stewards. (Application owners that control the content and quality of their applications' data)

1.1.13 **ICT Change Management Task Team:** The ICT Staff responsible to manage and guide the Change Control Processes.

1.1.14 **Computer Virus:** A computer program or script that interferes with, or damages the normal operation of a computer or any installed software. Virus programs are designed to infect other computers by hiding within e-mails or executable programs.

1.1.15 **Copyright:** Copyright is designed primarily to protect an artist, publisher, or other owner against any unauthorized copying of his works, by reproducing the work in any material form, publishing it, performing it in public, filming it, broadcasting it, causing it to be distributed to subscribers, or making any adaptation of the work. A copyright supplies a copyright holder with a kind of monopoly over the created material, which assures him of both control over its use and the pecuniary benefits derived from it.

1.1.16 **Emergency Maintenance:** Maintenance that requires to be performed to address and resolve a severity 1 or severity 2 issue.

1.1.17 **ETVX:** Entry-Task-Validation-Exit Model. **Entry criteria** – defines what must be provided or accomplished before the process can commence. **Tasks** is the sequence of steps to meet process objectives. **Validation** identifies the quality checkpoints in the process, and **Exit Criteria** identifies or describes the conditions that must be met before the process can be successfully terminated.

1.1.18 **Hardware Configuration:** Any component of a hardware platform, such as memory, mass storage, physical interfaces etc.

1.1.19 **Impact Analysis:** An examination of inter- and intra-system dependencies and the effects that will result from making a change. Impact assessments takes into consideration operational requirements (service level objectives, business operations, support etc), and how the change will affect other internal and/or external systems, subsystems, components, etc. An impact analysis of software configuration items used in a specific release or patch is called *build analysis.*

1.1.20 **Municipality:** Fetakgomo - Greater Tubatse Municipality.

1.1.21 **Post Implementation Validation:** A series of tests that take place after a change is made to the production environment, but prior to formal release to production. The goal of PIV is to exercise of major system or application subsystems and interfaces and to observe the system or application's stability and performance in the production environment prior to formally releasing the system or application into production (sustainment). The observation period with a real end users operating in the production environment is typically one hour. If no severity 1 or 2 issues occur during the observation period the implementation is deemed to be successful and the system or application is transferred to sustainment. If severity 1 or 2 issues occur during PIV the change is rolled-back. *Synonyms: Cycle 0 testing, sanity check, sanity test.*

1.1.22 **Quality Control:** A term used to describe the user acceptance or pre-production test functions, which are milestones in the system development life cycle. Often incorrectly called quality assurance. Software quality assurance is a proactive, metrics-based approach to software quality that monitors critical indicators at each stage of the system development life cycle, while quality control is a reactive, inspection-based approach to either hardware or software quality that occurs after the build milestone, but before the implementation (roll-out) milestone in the system development life cycle.

1.1.23 **Release:** The promotion of a change into the production environment and hand-off from development and implementation to sustainment. This is a critical milestone that occurs after a change has been implemented and has successfully passed the PIV checkpoint, and has been accepted by the BSM and application owner.

1.1.24 **Release Notes:** Software turnover documentation. Typically contains: List of deliverable items contained in the release (special instructions, updated documentation, media, scripts, executables, etc), description of release specifications, list of fixes/features, (by issue number of release), installation requirements and impacts, test results with remaining open issues and closed issues and any additional information to implement and support the product.

1.1.24 **Removable storage device:** A removable disk on which data may be stored. Usually refers to a Compact Disk or Flash Drive. For the purpose of this policy this term includes any removable storage device fitted to a personal computer.

1.1.25 **Requirements:** Initial stage in the system development life cycle during which functional and technical requirements are gathered. Requirements are the basis for design.

1.1.26 **Risk Assessment:** Identification of risks, their impact and methods or strategy to eliminate or mitigate the risks of their impact.

1.1.27 **Personnel:** Includes employees/staff/officials employed permanently and temporarily by Fetakgomo - Greater Tubatse Municipality.

1.1.28 **Severity:** A degree of impact a problem has on business operations. i.e.

(1) **Severity One** – Loss of application, or critical performance degradation with no workaround. Incident affects an entire workgroup.

(2) **Severity Two** – Moderate application degradation incidents. Severity one workaround. Incident affects several customers.

(3) **Severity Three** – Minor application degradation incidents. Incident or request has medium to high on single customers' ability to work.

(4) **Severity Four** – Incident or request has a low impact on single customers' ability to work.

1.1.29 **Staging Environment:** See production environment

1.1.30 **Downloading:** Acquiring (getting) a file /data from internet

1.1.31 **Hyperlink:** Automatic link to a URL

1.1.32 **Personal Account:** An account created on the computer for individual User for official usage

1.1.33 **URL:** Uniform Resource Locator, the address of a specific website

1.1.34 **User:** Authorised individual, making use of the Municipality IT Infrastructure

1.1.35 **ITD:** Information Technology Division, manned by the Manager: ICT, Senior Network Controllers; Network Controller, System Administrator and IT Technician.

1.1.36 **ISP:** Internet Service Provider.

1.1.37 **CD:** Compact Disk

1.1.38 **PAYDAY:** A payroll system used by Finance Department for salary administration

1.1.39 **E-Venus:** The financial system used by Fetakgomo - Greater Tubatse Municipality.

1.2 Purpose of the policy

This policy and procedures document sets forth Fetakgomo - Greater Tubatse Municipality's policy for making changes to production systems under the cognizance of the ICT Change Management Task Team, and explains the process and procedures for controlling changes in accordance with the policy.

1.3 Application of the policy

1.3.1 Objectives

1.3.1.1 To minimizing core system down time.

1.3.1.2 To control changes effected to critical systems.

1.3.1.3 To assign responsibilities for defined tasks.

1.3.1.4 To identify core software systems.

1.4 Scope of the policy

Change management policy and procedures are applicable to Fetakgomo - Greater Tubatse Municipality's ICT Unit.

CHAPTER 2
PROCEDURE STATEMENT

2.1 Change Control

It is the procedure of Fetakgomo - Greater Tubatse Municipality to manage the life cycle of all information systems supporting its business and technical objectives. As such, the processes and procedures for change control set forth in this document governs change, and release management. The scope of this document is the management of changes to the production environment. Specifically:

2.1.1 Before any change to a system or a baseline, the proposed change will be evaluated and approved by the Director Corporate Services.

2.1.2 No approved change will be implemented without:

2.1.2.1 A Change Control Management Request form has been duly completed and approved by the Director: Corporate Services.

2.1.2.2 A completed test plan showing the results of testing the change in a pre-production environment.

2.1.2.3 Approval from the application owner(s) affected by the change and the service provider responsible for the application or system being changed.

2.1.2.4 A formal review by Fetakgomo - Greater Tubatse Municipal ICT Unit to ensure that all Change Control Tasks as per the Change Control Management Request Form has been duly completed.

2.2 **FAILURE TO COMPLY**

Any system or application failure or defect traced to a change made to Fetakgomo - Greater Tubatse Municipal system or application that was not made in accordance with this process and procedures will result in disciplinary action. Specifically:

2.2.1 The error will be communicated to all stakeholders of the affected system and/or application.

2.2.2 Individual(s) making the unauthorized change will be required to develop an action plan specifying which measures will be taken to avoid a future occurrence of the failure or defect.

CHAPTER 3
CHANGE CONTROL PROCESSES

3.1 PROCESS

3.1.1 Software Applications and Process

The following software systems are subject to the Change Control Procedures:

3.1.1.1 Venus

3.1.1.2 PAYDAY Application

3.1.2 Documentation of Change Control Procedures

3.1.2.1 All relevant documentation and sign-offs must be completed as per prescribed procedure.

3.1.2.2 The procurement of software and related services is subject to the Supply Chain Policy.

3.1.3 Pre-production Environment and Testing

3.1.3.1 Pre-production Environment

3.1.3.1.1 All requests for change have to be tested on the pre-production environment of Fetakgomo - Greater Tubatse Municipality.

3.1.3.1.2 Changes such as patches, minor releases and version upgrades all need to be tested before roll-out on the production environment.

3.1.3.1.3 Proof of the test results have to be attached to the Change Control Request Form.

3.1.3.2 Test Results

3.1.3.2.1 Test results on the pre-production environment has to be documented on the Pre-Production Change Control Form.

3.1.3.2.2 In cases of major changes and upgrades the applicable service provider need to submit proof that the implementation of such changes were tested in their own environments.

3.1.4 Roll-back

3.1.4.1 In Pre-Production Environment

3.1.4.1.1 If a roll-back was needed during roll-out in the pre-production environment it needs to be documented and duly reported.

3.1.4.1.2 If and when the roll-back was executed due to mal functioning of the systems, the change may not be rolled out on the production environment until the exact cause for the system failure has not been established and reported.

3.1.4.2 In Production Environment

3.1.4.2.1 If and when a change effected have negative results on the production environment a roll-back needs to be executed.

3.1.4.2.2 The system should be restored to its original state.

3.1.4.2.3 ICT Staff responsible should use the full system back-up performed before the actual change to restore the affected data.

3.1.4.2.4 If and when a roll back on the production environment occurred, it should be well documented and the cause of the system failure should be determined by the service provider.

3.1.4.2.5 Before another attempt can be made to roll-out the change, the service provider needs to provide proof that steps were taken to mitigate a re-occurrence of the system failure.

3.1.5 Process Description

The change control process is depicted in the following diagram:

3.2 PROCEDURES

3.2.1 CHANGE INITIATION

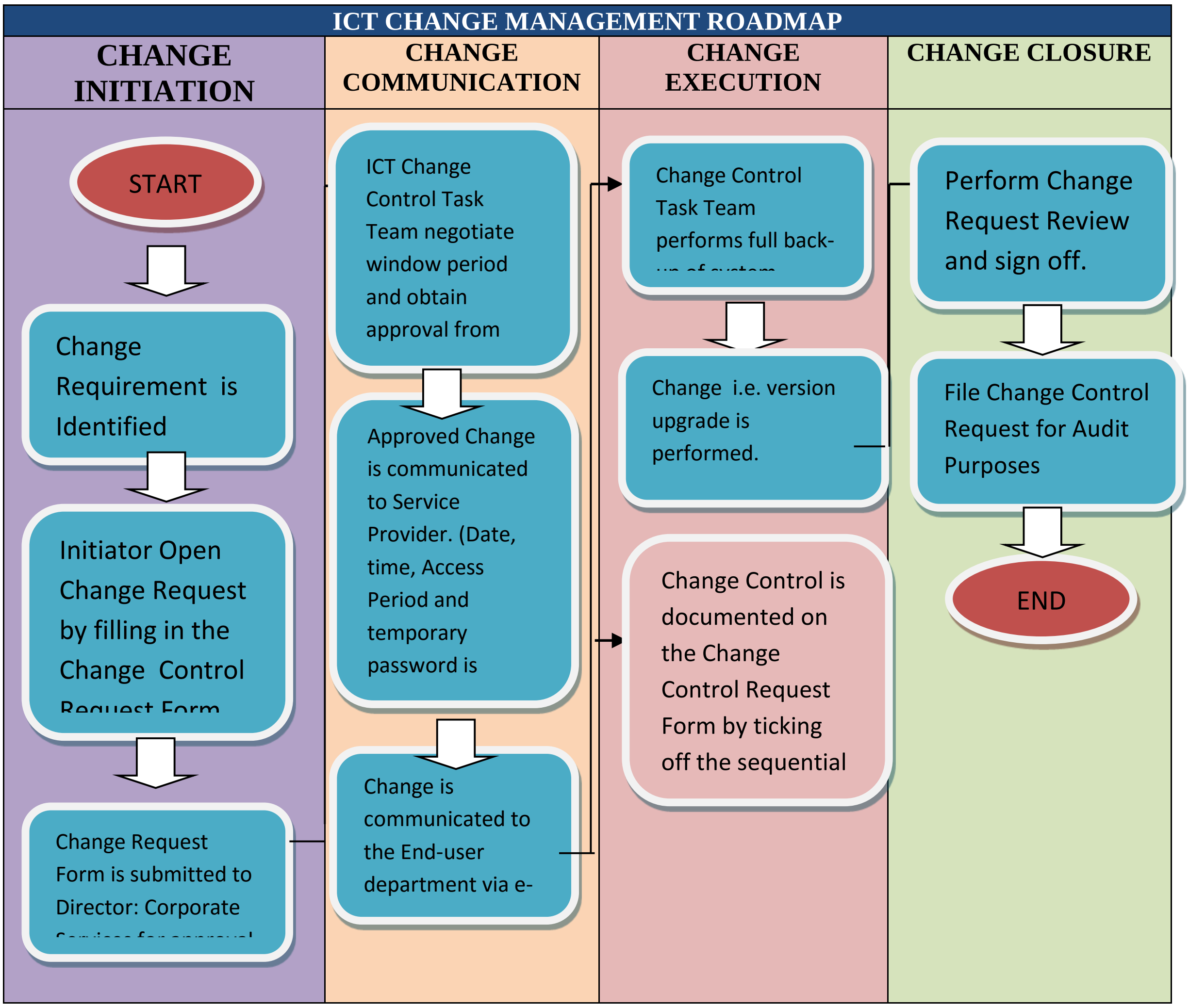
3.2.1.1 Change Requirement

The Change Requirement is usually identified by the Initiator of such change. The Initiator can be an end user, application owner or service provider of the system.

3.2.1.2 Open Change Request

The Initiator opens a Change Request by filling in the Change Control Request Form.

3.2.1.3 Approval and Authorization


ICT CHANGE MANAGEMENT ROADMAP
CHANGE INITIATION
CHANGE COMMUNICATION
CHANGE EXECUTION
CHANGE CLOSURE
START
Change Requirement is Identified
Initiator Open Change Request by filling in the Change Control Request Form
Change Request Form is submitted to Director: Corporate
ICT Change Control Task Team negotiate window period and obtain approval from
Approved Change is communicated to Service Provider. (Date, time, Access Period and temporary password is
Change is communicated to the End-user department via e-
Change Control Task Team performs full back-
Change i.e. version upgrade is performed.
Change Control is documented on the Change Control Request Form by ticking off the sequential
Perform Change Request Review and sign off.
File Change Control Request for Audit Purposes
END

3.2.1.3.1 The Change Request is submitted to the Director: Corporate Services for approval.

3.2.1.3.2 The function of Change Control is the responsibility of the Director: Corporate Services.

3.2.1.3.3 The Director might sub-delegate the function in writing to his appointed subordinate.

3.2.1.3.4 In the case of any changes to the delegation, written instructions must be issued.

3.2.1.3.5 If a change has not followed the agreed procedure, the matter must be investigated. This could take the form as an inquiry, a formal internal investigation or an independent investigation. The Director: Corporate Services will rule on the type of investigation as well as acceptance of the report.

3.2.1.3.6 If other systems are affected, all the relevant staff must be informed and must agree to the change.

3.2.2 CHANGE COMMUNICATION

3.2.2.1 Window Period

3.2.2.1.1 The window period needs to be negotiated with the end-user department and/or application owner of the system.

3.2.2.1.2 Once agreement has been reached approval from the Manager of the Department is obtained via signing on the Change Control Request form.

3.2.2.1.3 When negotiating the window period, the ICT Staff need to factor in the period required for a possible roll back in case the change i.e. version upgrade is not successful.

3.2.2.2 Communication to Service Provider

3.2.2.2.1 The agreed upon date, time, period of down time (access period) and temporary password is communicated to the applicable service provider via e-mail.

3.2.2.2.2 Responsible ICT Staff has to ensure that the password is revoked after the window period lapsed.

3.2.2.2.3 Proof of communication should be attached to the Change Control Request form.

3.2.2.3 Communication to End Users

3.2.2.3.1 ICT Staff has to communicate the planned changed as agreed upon to all effected end-users at least 1 day in advance via e-mail.

3.2.2.3.2 ICT staff responsible for the Change Control needs to ensure that proof of the communication is attached to the Change Control Request form.

3.2.3 Change Execution

3.2.3.1 System Back-up

3.2.3.1.1 The ICT Staff is responsible for making a full system back-up prior to the change being rolled out.

3.2.3.1.2 Proof of the full system back-up needs to be attached to the Change Control Request Form.

3.2.3.1.3 The requested change may not commence before this step has not been executed.

3.2.3.1.4 Failure to comply with this step will lead to disciplinary action.

3.2.3.2 Change Execution

3.2.3.2.1 Once a full system back-up has been performed and proof thereof has duly been attached to the Change Control Request Form the change is rolled out or executed.

3.2.3.2.2 During the change ICT Staff needs to monitor the progress of the process and should be in a position to execute the roll-back if so required.

3.2.4 Change Closure

3.2.4.1 Change Request Review

3.2.4.1.1 Once the requested change has been executed successfully, the review process begins by submitted the Change Control Request Form together with all applicable attachments to the Manager: ICT.

3.2.4.1.2 The Manager: ICT ensures that all sequential steps have been performed as per the Task List on the Change Control Request form.

3.2.4.1.3 The Manager: ICT forwards the completed Change Request Form to the Director: Corporate Services for final signature.

3.2.4.2 Filing of Change Requests

3.2.4.2.1 The ICT Staff responsible for the Change Request Execution have to duly file the completed Change Control Request forms orderly in a file for that purpose.

3.2.4.2.2 The file should be presented to the Auditor General if and when requested to do so.

CHAPTER 4
HARDWARE CHANGES

4.1 All hardware changes are subject to the approved Standard Specifications which stipulates the base for all hardware configurations.

4.2 The Standard Specifications will be reviewed once a year and updated as required in line with the Global ICT Policy.

4.3 The appropriate Supply Chain Policies will apply to hardware acquisitions.

4.4 All hardware installations are subject to the related procedures as approved, and are subject to the Backup Policy, Disaster Recovery Plan and all other related policies and procedures.

CHAPTER 5
PLANNED MAINTENANCE

5.1 Planned maintenance is by definition a scheduled event. Users must be informed timeously about the schedule and the impact thereof.

5.2 As a general rule no maintenance will be completed during normal working hours.

5.3 The only time that item 5.2 above can be overridden is when a critical event has occurred on the system and which adversely affects the operation of the system.

5.4 Only the Director: Corporate Services can approve such changes. Users must be informed of these events as soon as possible.

CHAPTER 6
EMERGENCY MAINTENANCE/CHANGES

6.1 Emergency maintenance is by definition maintenance that was not planned and/or scheduled and occurs in an event where the functionality of the system is adversely affected.

6.2 Emergency maintenance can occur either in working hours and/or after hours.

6.3 In case of an emergency maintenance verbal approval from the Director: Corporate Services for the maintenance will be sufficient, where after an emergency maintenance report should be prepared by the applicable Service Provider providing details on the cause of the fault as well as the remedial action taken.

6.4 Emergency maintenance and changes should be well documented to ensure that preventative maintenance, if possible is planned and documented for future reference.

6.5 Severity one cases includes incidents when there is loss of application, or a critical performance degradation with no workaround. These incidents usually affect an entire workgroup.

6.6 Severity Two cases include incidents when there is moderate degradation with a workaround. These incidents usually affect several end-users.

CHAPTER 7
CHANGE OF ACCESS RIGHTS TO DOMAIN AND/OR SYSTEMS

7.1 Change of access rights occur when:-

7.1.1 An employee has been promoted from one position to another.

7.1.2 An employee was demoted from one position to another and/or when an employee’s conduct is questionable with regard to the safe guarding of confidential information of Fetakgomo Tubatse Municipality.

7.2 The ICT Division on a written request received by the HR Department accompanied with the User Account Form will change the access rights of an employee to the Domain and/or other ICT Systems as per the request received.

7.3 The User Account Form should be filed on the personal file as well as the ICT Unit’s files of such employee for later reference and audit queries if needed.

CHAPTER 8
POLICY REVIEW AND VERSION CONTROL

8.1 Policy Review

This Policy shall be reviewed twenty four (24) months after the day of approval.

8.2 Version control

Development Date	
Developed by:	
Version:	