CHRIS HANI
DISTRICT MUNICIPALITY
SUSTAINING GROWTH
THROUGH OUR PEOPLE

SYSTEMS PROGRAM CHANGE MANAGEMENT POLICY AND PROCEDURE

2026/2027

Adopted in an Ordinary Council meeting held on 27 May 2026.

Table of Contents

1. Problem Statement 3
2. Purpose 3
3. SCOPE 3
4. Legislative Framework 3
5. DEFINITIONS 4
6. POLICY 5

6.2 Change Planning, Evaluation and Scheduling 5
6.3 Test Environment 5
6.4 Change Testing 6
6.9 Change Implementation 9
7. RESPONSIBILITY 110
8 Training And Awareness 11
9. COMPLIANCE 12

1. Problem Statement

Lack of change control environment to manage, record and track all changes within ICT environment in CHDM.

2. Purpose

The purpose of this policy is to ensure there is a business reason for each change, identifying the specific configuration items and IT services affected by the change, identifying those responsible for implementing the change, planning the change, testing the change and having a back-out plan should the change result in an unexpected failure.

3. SCOPE

This policy applies to all Chris Hani District Municipality employees, contractors and any other individuals involved in making changes to Chris Hani District Municipality's services for which IT has accountability.

4. Legislative Framework

- ISO20000, service management standard
- 27001 information security standards,
- Information Technology Infrastructure Library (ITIL) and
- COBIT 2019

5. DEFINITIONS

Change: A change is any activity that occurs to any information resource where the status is different from a previously defined condition. This is applicable to all IT hardware, communications equipment and software, business systems software, 'live' applications software and all documentation and procedures that are relevant to the running, support and maintenance of live systems. A change can also be initiated to resolve a critical problem.

User (s): For the purposes of this document any reference to 'user' or 'users' is referring to the business users who initiate the change request.

Emergency Change: An emergency change is an unexpected or unplanned change that will either minimise service disruption or restore service.

Change Management is the process of developing a planned and documented approach to change in an organisation.

In the ITIL framework, Change Management is responsible for controlling change to all configuration items within the live environment, test and training environments, and all environments under the control of 'IT Operations'.

Business owner: Manager of an organisational unit within Chris Hani District Municipality who bears responsibility for the acquisition, development and maintenance of production applications that process municipality information.

Configuration Items: A component within a system configuration that needs to be controlled.

ITIL: United Kingdom's Office of Government Commerce Information Technology Infrastructure Library.

6. POLICY

Every change to Chris Hani District Municipality's IT services is subject to the IT Change Management Policy and must follow the approved Chris Hani District Municipality IT Change Management Procedure.

6.1 Change Requests

6.1.1 A formal change request process must be initiated to ensure that any changes follow a defined change process for all types of changes.

6.1.1 All changes requests must follow an up-to-date Change Management procedure.

6.2 Change Planning, Evaluation and Scheduling

6.2.1 All changes must be planned, evaluated and scheduled.

6.2.1 A risk and impact analysis of the change must be performed and included in the planning and evaluation of change requests to ensure that all components and risks affected by the change have been identified and assessed.

6.2.2 A back-out plan must be documented for all changes.

6.3 Test Environment

6.3.1 The Chris Hani District Municipality must use a secure test environment that is representative of the production environment. If the municipality cannot afford to build test environments, a virtual test environment must be provisioned.

6.3.2 The IT Management must ensure that the test environment cannot interact with production systems.

6.4 Change Testing

6.4.1 Testing of changes must be performed prior to the change being implemented in the production environment and proof of testing must be retained as evidence. Systems such as Payday and Solar, service provider, must provide test results for each version change before it is implemented in a production environment.

6.4.2 **Planning and Testing:** All version updates must undergo formal **planning**, **risk assessment**, **testing**, and **validation** before being deployed to production. This will include compatibility testing and regression testing to ensure the updated version functions as intended in the live environment.

6.4.3 **Approval Process:** Ensure version updates are submitted to the **Change Advisory Board** for formal review and approval prior to deployment.

6.4.4 **Test Results from Service Providers:** Service providers must provide comprehensive **test results** before version updates are approved for production deployment. These results should include:

6.4.5 A list of tests performed (functional, security, performance).

6.4.6 Test outcomes and any issues identified.

6.4.7 Details of how issues were addressed.

6.5 Migration of Changes to Production

- **6.5.1 Change Implementation** should be updated to explicitly include processes for the migration of changes to production:

- All changes must undergo **thorough testing** and **validation** in a **secure test environment** before being migrated to the production environment.
- **Approval workflows** for production changes must be clearly defined and documented, including sign-off from the relevant stakeholders (e.g., Change Advisory Board, business owners, and technical teams).
- Formal approval of changes based on documented testing, risk analysis, and impact assessment. This approval must include a detailed sign-off for each change before it is deployed to production.
- **Test Results from Service Providers**: Service providers must provide comprehensive test results before version updates are approved for production deployment. These results should include:
- A list of tests performed (functional, security, performance).
- Test outcomes and any issues identified.
- Details of how issues were addressed.
- All unsuccessful changes must be rolled back in accordance with the defined rollback plan.

6.6 Segregation of Duties

- **Separate responsibilities** for development, testing, approval, and deployment of changes. Specifically:
- Developers may implement changes but **cannot approve** or deploy them.
- Testers are responsible for validating the changes but **cannot approve**

the deployment.

- A separate **Change Advisory Board (CAB)** or relevant authority must review and approve all changes before deployment into production.
- IT Management should conduct a **root cause analysis** to understand why change control logs were not available, investigating issues with system configurations, process gaps, or human error.
- **Change Log Maintenance** should be logged which mandates the creation and maintenance of **comprehensive change control logs** for all changes. These logs should include detailed records of the change request, approval process, testing results, deployment actions, and post-implementation reviews.
- A **central repository** must be used to store change logs, making them accessible for future audits and reviews.

6.7 Change Documentation

- Change Documentation should emphasize that failure to maintain proper change logs is a serious compliance issue, and management must address repeat findings with senior leadership to ensure that logs are maintained, tracked, and retrievable for audits.

6.8.1 Change Reporting

6.8.2 Use of **automated change management tools** to track all changes, including approval workflows, testing results, and deployment statuses.

6.8.3 **Audit logs** that capture all actions performed within the change management system (e.g., initiation, approval, deployment) for future review and accountability.

6.8.4 **Regular reviews** of changes made to production systems, including post-implementation reviews and audits of all changes for unauthorized or unapproved changes.

6.8.5 The IT Management must monitor open changes to ensure that all approved changes are closed in a timely fashion.

6.8.5.1 The IT Management must maintain a tracking and reporting system for all change requests.

6.9 Change Implementation

6.9.1 Change Advisory Board must formally approve each change request prior to the implementation of the change in the production environment.

6.9.2 All changes must be communicated with the relevant stakeholders prior to implementation in the production environment.

6.9.3 All unsuccessful changes must be rolled back in accordance with the defined rollback plan.

6.10 Emergency Changes

6.10.1 A procedure must exist to govern emergency changes to information systems and related technology.

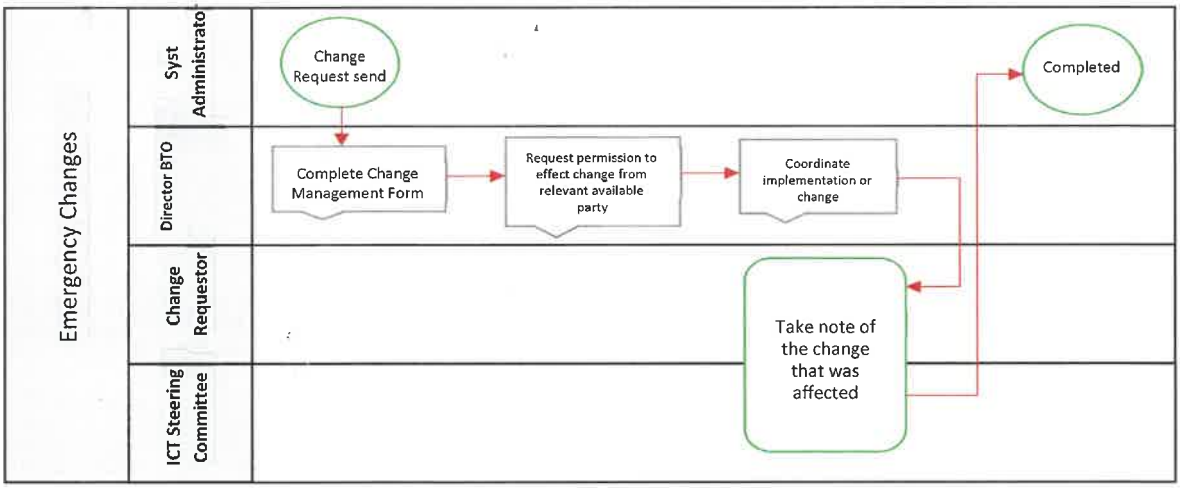
6.10.2 Criteria that define an emergency change must be clearly documented and communicated.

6.10.3 Emergency changes must be documented.

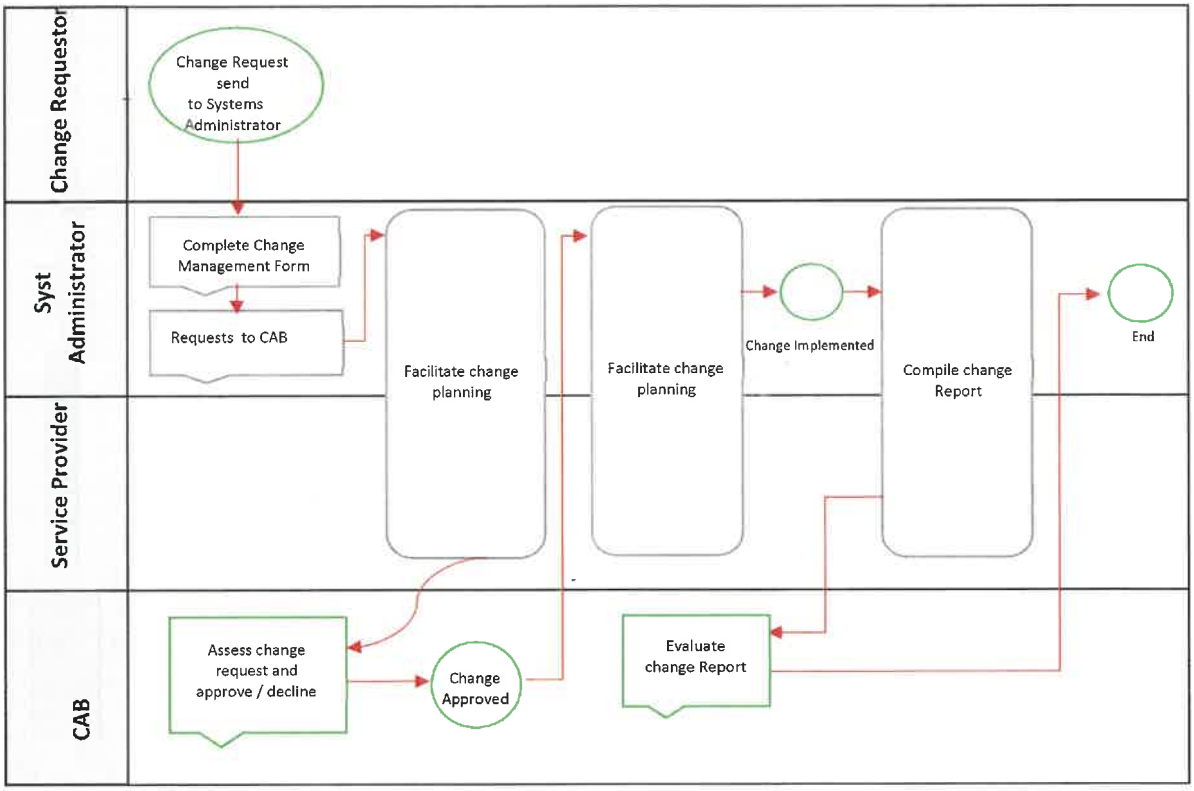
6.10.4 Emergency changes must be approved by Emergency Change Advisory Board.

6.10.5 Emergency Changes should be updated to include more robust controls and procedures for emergency changes, ensuring that emergency changes are documented, tested, and approved to the same standards as regular changes.

EMERGENCY WORKFLOW:



STANDARD WORKFLOW:



6.5 7.RESPONSIBILITY

All employees, contractors, business owners are required to adhere to this policy. Non-compliance to this policy may lead to appropriate disciplinary action.

8.TRAINING PLAN AND AWARENESS

8.1 All business owners and managers are responsible for promoting individual employee awareness of and compliance with the municipality's IT Change Management policies and procedures.

8.2 Mandatory training for all individuals involved in the change management process to emphasize the importance of segregation of duties and compliance with updated change management policies.

8.3 Ongoing education on how to use change management tools, ensuring staff members are trained in proper documentation, approval processes, and the importance of secure change migration.

8.4 After the policy updates are approved, communicate the changes to all stakeholders involved in the change management process. Conduct training sessions for relevant personnel on the new procedures, particularly focusing on segregation of duties, version updates, and maintaining change logs.

6.6 9.COMPLIANCE

All employees, contractors, business owners must comply. All exceptions to this policy must be done via approval of the Municipal Manager.

Review of the policy

This policy must be reviewed at least annually or when the need arises.

EFFECTIVE DATE

This Policy takes effect on the 01st of July 2026

Policy Adopted the Chris Hani District Municipality council meeting; dated

Council Resolution:

Resolution No: C163

2026-2027.

Signed by Municipal Manager: G. Mashiyi — ***Initial and Surname*** — ***Signature*** — 09/06/2026 — ***Date***

Signed by Speaker of Council: J. Cengani — ***Initial and Surname*** — ***Signature*** — 09/06/2026 — ***Date***