DRAKENSTEIN
MUNISIPALITEIT • MUNICIPALITY • UMASIPALE WASE
"A Place of Excellence"

"

# Change Management Policy

| APPROVED/REVIEWED | COUNCIL MEETING DATE |
|---|---|
| March 2017 / March 2020 | 29 March 2017 |

**TABLE OF CONTENTS**

## 1. PREAMBLE

Information systems and technology is increasingly used as an enabler of the business of the municipality in fulfilling its strategic mandate. Due to the nature of the mandate municipality there are both critical business and peripheral information systems in use.

These information systems facilitate delivery of processes, human intervention with these processes and the information carried within them. Inevitably the business critical information systems have grown to become a core engine to the business of the municipality.

It is thus important that all effort be expended by the municipality to ensure that the ICT enabled business processes not be interrupted or compromised in any way. This policy sets measures in place to ensure that process and information are protected against possible risks.

The risk environment that is mitigated by the implementation of this policy addresses inter alia:

- Uncontrolled and unplanned changes made to the ICT environment and information systems lead to the breakdown in processes or compromise information;
- Protect information against breakdown in functionality of information systems and ICT infrastructure; and
- Uncontrolled changes lead to exploitation of information carried within automated processes.

Information and communication technology (ICT) change management institutes a discipline and quality control in the form of planning, evaluation, review, approval, communication, implementation, documentation and post mortem activities in the form of rules and processes.

This positions the municipality to facilitate efficient and effective control of changes and introduction of new technology and solutions in the ICT environment. The change management processes, approval structures and controlled implementation ensure protection of the business of the municipality. It positions information system owners and ICT management to demonstrate increased agility in responding predictably and reliably to new business demands.

This policy will ensure the implementation of change management and control strategies to mitigate associated risks such as:

- The business unable to render normal information system based services;
- Inability to retrieve or access historical information required to serve the public;
- Decrease in productivity reverting back to manual transactions;
- Degrading management practices;
- Reduction in turnaround times;
- Lapse or breach in information security;
- Productivity losses; and
- Exposure to reputational risk.

## 2. 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.

## 3. DEFINITIONS

| Terminology | Definition | Abbreviation |
|---|---|---|
| | | |
| Change management | Refers to the standard practice to manage in an information technology environment. | |
| Change Management Committee | The committee responsible for the evaluation of change requests and its denial or approval. | CMC |
| Change Plan | The plan that indicates how the change will be effected, risks and their impact and which rollback procures will be used if unsuccessful. | |
| ICT cloud | It is an Internet-based computing platform that provides shared computer processing resources and data to computers and other devices on demand | |
| Electronic information | Refers to information created by, stored within and manipulated via electronic means. | |

| Terminology | Definition | Abbreviation |
|---|---|---|
| Information and communication technology | An extended term for information technology (IT) which stresses the role of unified communications[1] and the integration of telecommunications (telephone-lines and wireless signals), computers as well as necessary enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information | ICT |
| Information security | Is the practice of protecting electronic information against unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. | InfoSec |
| Information systems | Refers to the technology systems used to collect, filter, process, create and distribute data. | |
| | | |

## 4. SCOPE

This policy applies to all staff and line function units, ICT related service providers, ICT department and users of electronic information resources within the municipality. It addresses planned changes to all forms of authorised information and communication systems and infrastructure located in the offices of the municipality and those housed by service providers. It applies to all temporary, contracted or fulltime employees, service providers and advisors that is granted access to the Drakenstein domain and/or applications and information systems and related infrastructure owned by or contracted for the use of the municipality.

## 5. PURPOSE

The purpose of this policy is to establish management direction and high-level objectives for change management and control with regards to the Drakenstein domain and related information systems.

## 6. POLICY

### 6.1 Changes to ICT resources

Changes to ICT information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are:

- **Documented:** Document (process, culture, cloud, application and back office configuration and architectural implications) the change and any review and approval information.

- **Planned:** Plan the change, including the **implementation design, scheduling, test plan** (where possible) **and roll-back plan**.
- **Evaluated:** Evaluate the change, including determining the **priority level** of the service and the **risk of the proposed change**; determine the change classification and the change process to be used.
- **Reviewed:** Review change plan with peers and/or Change Management Committee (CMC) as appropriate to the change type.
- **Approved:** Obtain approval of the CMC as needed.
- **Communicated:** Communicate change with the appropriate parties.
- **Implemented:** Implement the change.
- **Post-change reviewed:** Review the change projecting towards future improvements.

In order to fulfil this policy, the following rules shall be adhered to:

## 6.2 Application for and Approval of Change Request

### 6.2.1 Standard Changes

*6.2.1.1 Rule*

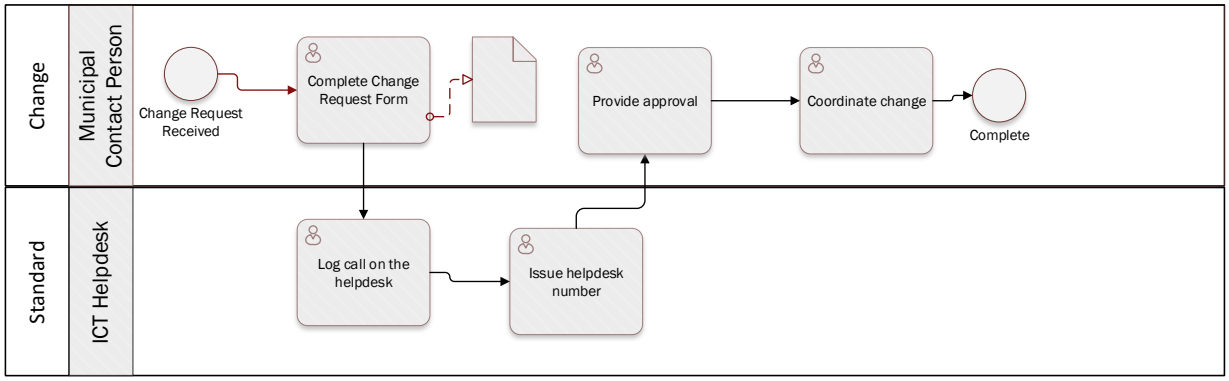
A change request shall be handled according to the following procedure:

- The requestor completes the change request form (**Annexure A**);
- The completed form is provided to the municipal contact person for the specific information system i.e. SOLAR – Senior Operator and Resourcelink – Manager Financial Services;
- Contact person logs the change request on the ICT helpdesk and obtains helpdesk reference number;
- The contact person provides approval for the roll-out of the change;
- The contact person monitors that the change was applied.

**Note:** In the case of standard changes that are approved by the CMC (See Annexure B), which will be revised as and when required but a least annually, the change request form is not completed. The responsible person will log a call on the helpdesk and coordinate that the change is applied.

### 6.2.2 Process:

The following process applies:



### 6.2.3 Control:

- Completed and approved change requests, where applicable; and
- The Chairperson of the CMC validates that appropriate controls are applied on a six monthly basis.

### 6.2.4 Significant Changes

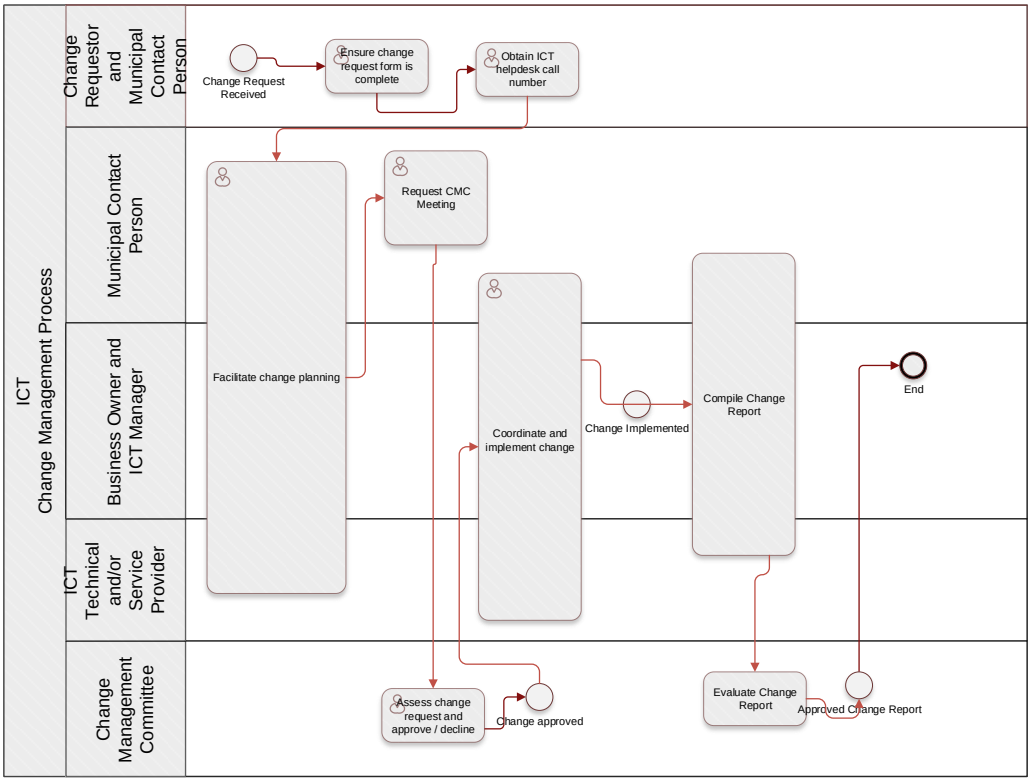
*6.2.4.1 Rules:*

A change request shall be handled according to the following procedure:

- The requestor completes the change request form (**Annexure A**);
- The completed form is provided to the municipal contact person for the specific information system i.e. SOLAR – Senior Operator and Resourcelink – Manager Financial Services;
- Contact person logs the change request on the ICT helpdesk and obtains helpdesk reference number;
- The call is routed to the Chairperson of the CMC (Senior Manager ICT) to arrange ad-hoc change management meetings;
- Senior Manager ICT routes request to the appropriate official to plan and present the change at the CMC;
- Responsible official facilitates planning of the change;
- The change impact, risk of the change, the change implementation plan and process for roll-back serves at the CMC for evaluation and approval;
- The CMC shall consider risk and impact with regards to the change request and approve or disapprove;
- The relevant official coordinates implementation;
- Change report is drafted; and
- CMC accepts change report.

### 6.2.5 Process:

The following process applies:




### 6.2.6 Control:

- Completed and approved change requests and reports.

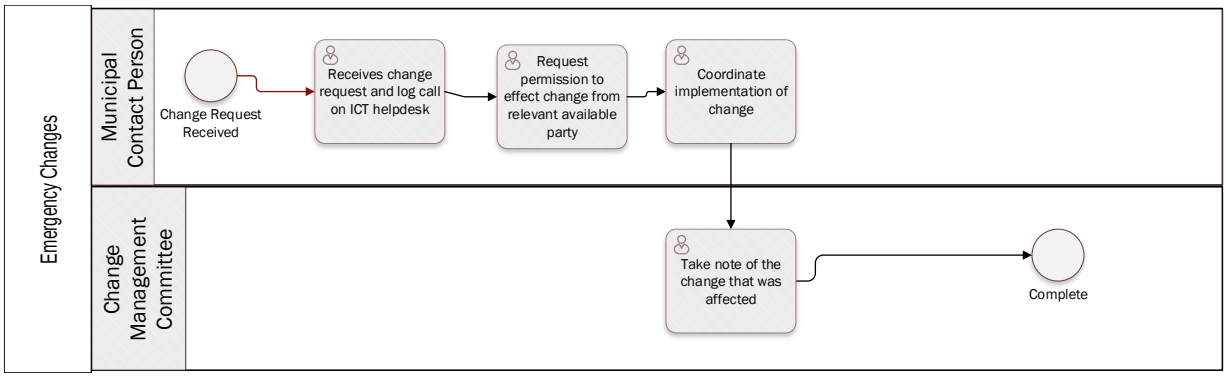
### 6.2.7 Emergency Changes

*6.2.7.1 Rule*

- Requestor completes the change request form.
- The municipal contact person logs the change request on the ICT helpdesk and obtains helpdesk reference number.
- The municipal contact person request approval to affect change from the relevant party verbal, short message service or e-mail.
- The municipal contact person coordinates the implementation of the request.
- The municipal contact person sends an e-mail to support@drakenstein.gov.za to log a call on the helpdesk.
- The helpdesk issues a call number.
- The municipal contact person routes the request, call number and relevant documentation to the chairperson of the CMC to organise and ad-hoc meeting.
- At the CMC meeting the relevant information for the completed request is noted and where necessary feedback provided to all roll players.

### 6.2.8 Process:

The following process applies:




### 6.2.9 Control:

- Completed and approved change requests and reports.

## 6.3 Change Classification

All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on business and ICT operations according to the following guidance:

- **Standard Change** – A low-risk change with well-understood outcomes that is regularly made during the course of normal business. A Standard change follows pre-determined processes, is pre-approved by the CMC and may be made at the discretion of the municipal representative, Senior Manager ICT, Executive Manager Corporate Services or Municipal Manager. Standard changes will be revised on an annual basis. A list of standard approved changes is attached as **Annexure B**.
- **Significant Change** – A significant change is one that has results in a change of mission critical information systems (Financial and Human Resource and other core systems), it involves less understood risks, has less predictable outcomes, and/or is a change that is not regularly made during the course of business. Because of the ability to affect downstream or upstream business services, any proposed significant change must be authorised by the CMC.
- **Emergency Change** – this is similar to a significant change, but must be executed with utmost urgency. There may be fewer people involved in the change management process review, and the change assessment may involve fewer steps, but any emergency change must be approved by the Staff and/or Line Function Senior Manager, Senior Manager ICT, Executive Manager Corporate Services or the Municipal Manager.

With regards to classified changes, the CMC can, from time-to-time update the list of standard changes as deemed necessary.

## 6.4 Change request information required:

### *6.4.1 Infrastructure:*

Infrastructure refers to all identifiable elements of the Drakenstein domain. This includes data links (terrestrial and radio), domain technology (servers, routers and switches), database and software systems that facilitates the provisioning and operations of the domain and any other technology implemented that provisions the service to the user-base and where allowed service providers. These change requests should take the following into consideration:

- Description of the environment within which the change is requested;
- Impact on technology, processes and standard operating procedures;
- Impact on skills and competency requirements;

- Purpose of the change requested;
- Risk of the change requested; and
- Impact on the ICT Business Continuity Plan.
- Change control form is attached as **Annexure A**.

### *6.4.2 Application, cloud back-end information change request:*

This encompasses any information/application systems (regardless of where it is housed) that are used to provide presentation layer interfaces to the user and includes the appropriate back-end systems used to manage the data of these (i.e. databases and middleware). In this regard the change request should take the following in consideration:

- Information system in which the change is requested;
- Purpose of the information system;
- Business processes impacted and its implications;
- How the change will relate to change in business processes;
- Business culture change requirements and management;
- For systems housed in-house: Related information system change requirements in terms of: database systems, application systems, integration with other systems, infrastructure and underlying operating system requirements;
- For systems housed in the cloud: Integration with other systems, infrastructure and underlying operating system requirements; and
- Impact on the ICT Business Continuity Plan.
- Change control form is attached as **Annexure A**.

### *6.4.3 Cloud Based Information System*

These are information systems that are housed by the service provider within its private hosting space (cloud) and are managed through a service level agreement between the staff and line function and the supplier. These suppliers are expected to inform the municipality of a change that will be performed and when the change will be implemented. Furthermore, these kind of change requests will only serve to inform the CMC of the intention of the supplier to perform the change. In this regard, the following should be taken into consideration:

- What the business uses the information system for;
- Impact on business process and how it will be changed; and
- Business culture change requirements and management.
- Change control form see attached as **Annexure A**.

## 7. COMPOSITION OF THE CHANGE MANAGEMENT COMMITTEE (CMC)

The CMC shall comprise of the following members:

- Senior Manager ICT (Chair Person);
- ICT Governance and Administration Manager;
- Information Systems Manager;
- Operations and Support Manager;
- Staff and/or Line Function Senior Manager or Manager;

- Where a service level agreement (SLA) is involved, a representative of the service provider; and
- Any other role player that may be co-opted from time-to-time.

## 8. PLANNING OF CHANGES

### 8.1 Change Plan

All changes, except standard changes, should be planned and reflect as a minimum the following:

- What will be changed;
- Role-players and their responsibilities;
- When will the change take place;
- Implementation plan;
- Version control;
- Rollback plan; and
- Impact on the ICT Continuity Plan.

### 8.2 Testing of Proposed Changes

Changes shall, where possible, be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation. This is done in order to minimise the impact on business and information system security. Where requested changes cannot be tested the CMC should be satisfied that the proposed changes do not pose an unnecessary risk to the business functionality or ICT infrastructure and information systems environment.

### 8.3 Change register

A change register shall be maintained by the Senior Manager: ICT.

## 9. CONTROLS

The following controls apply:

- List of standard changes shall be approved by the CMC;
- All change requests are recorded in the change control register;
- The change control register will be signed by the Manager ICT Governance and Administration on a quarterly basis and Senior Manager ICT six monthly.

## 10. COMPLIANCE

Any person, subject to this policy, who fails to comply with the provisions as set out above or any amendment thereto, shall be subjected to appropriate disciplinary action in accordance with the Disciplinary Code.

## 11. RETENTION OF CHANGE MANAGEMENT DOCUMENTATION

Change management documentation will be retained in accordance with the requirements of the relevant information system.