# ICT Change Management Policy

# V2.0

| APPROVED/REVIEWED | COUNCIL MEETING DATE |
|---|---|
| 27 October 2020 | 27 October 2020 |

# Table of Contents

## Document Identification

| | |
|---|---|
| **File Name** | ICT Change Management Policy |
| **Version** | Version 2.0 |
| **Sensitivity Classification** | Client Confidential Information |
| **Document Owner** | Laingsburg Municipality |

## Preparation

| Action | Name | Role/Function | Date |
|---|---|---|---|
| Prepared by: | Realdo Pedro | ICT Administrator | 06\05\2019 |
| Reviewed/Approved by: | Realdo Pedro (Reviewed) | ICT Administrator | 21\09\2020 |

## Release

| Version | Data Release | Change Notice | Remarks |
|---|---|---|---|
| 1.0 | 06\05\2019 | Created and Drafted Realdo Pedro (ICT Administrator) | None |
| 1.1 | 09\03\2020 | Reviewed and prepared for approval Realdo Pedro (ICT Administrator) | None |
| 2.0 | 21\09\2020 | Reviewed with ICT DLG Western Cape (via MS Teams) | None |
| 2.0 | 27\10\2020 | Approved By Council | Policy approved without any remarks |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 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 as a result of uncontrolled changes being implemented in the ICT environment.

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 that could lead to the malicious use and manipulation of information by unauthorised person(s).

Information and communication technology (ICT) change management institutes a discipline and quality control when planning, evaluating, reviewing, approving, and communicating the implementation of ICT changes.

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. DEFINITION

| Terminology | Definition | Abbreviation |
|---|---|---|
| | | |
| Change Management | Refers to standard Practice to manage changes in an information technology environment. | |
| ICT Steering 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. | |
| 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 |

| Terminology | Definition | Abbreviation |
|---|---|---|
| | | |
| 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 Laingsburg 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 Laingsburg 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, and 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*

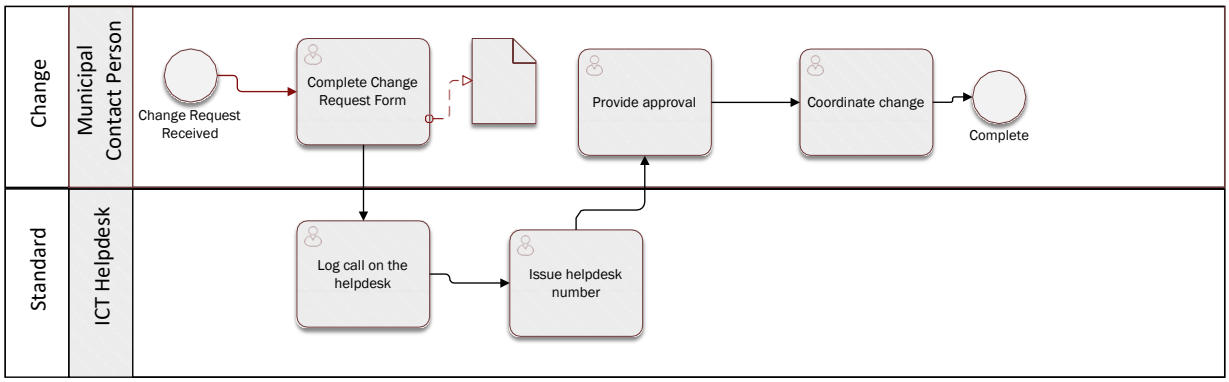
A change request shall be handled according to the following procedure:

- 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 Resource link – 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

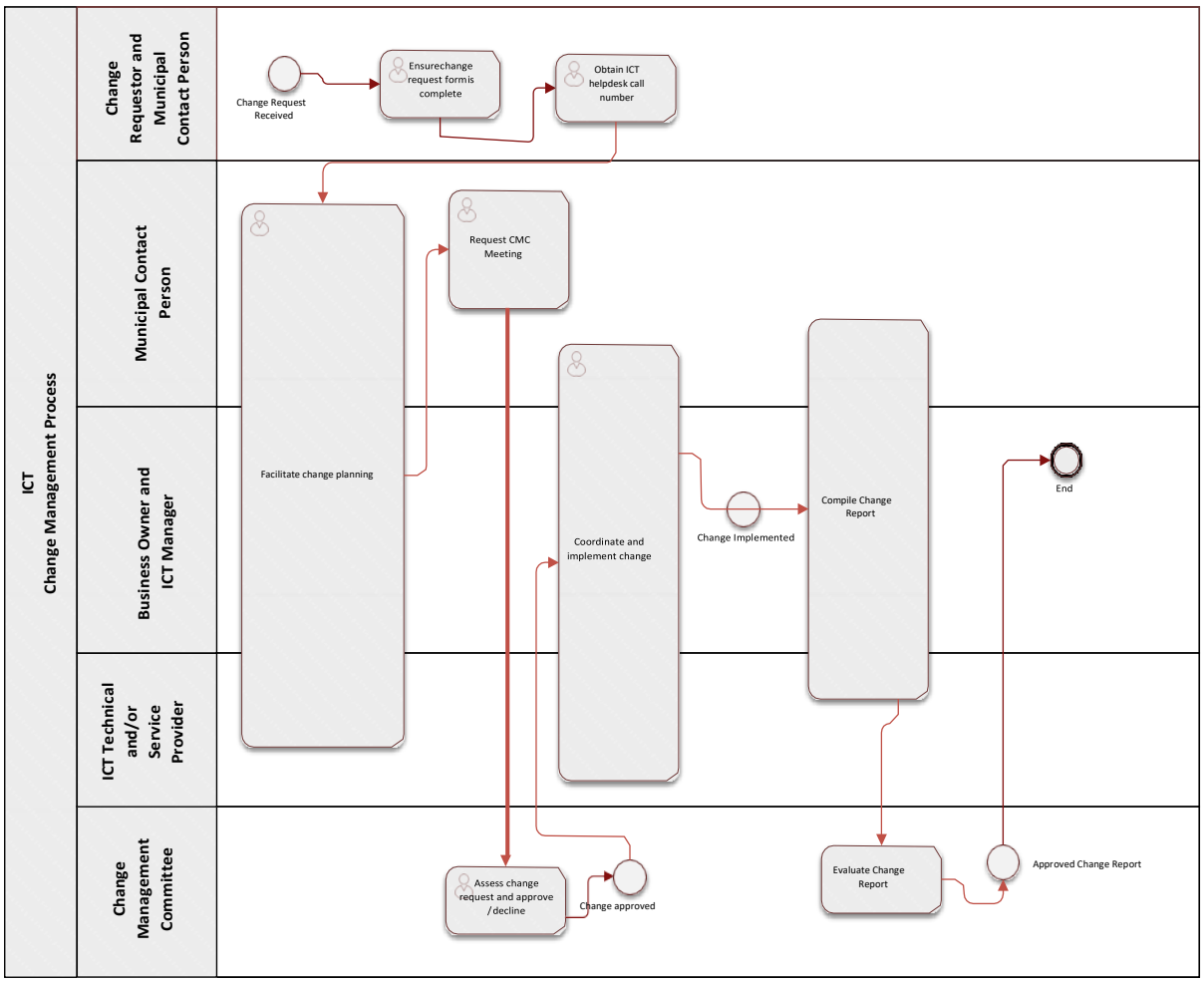
6.2.4.1. Rules:

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 Resource link – 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.

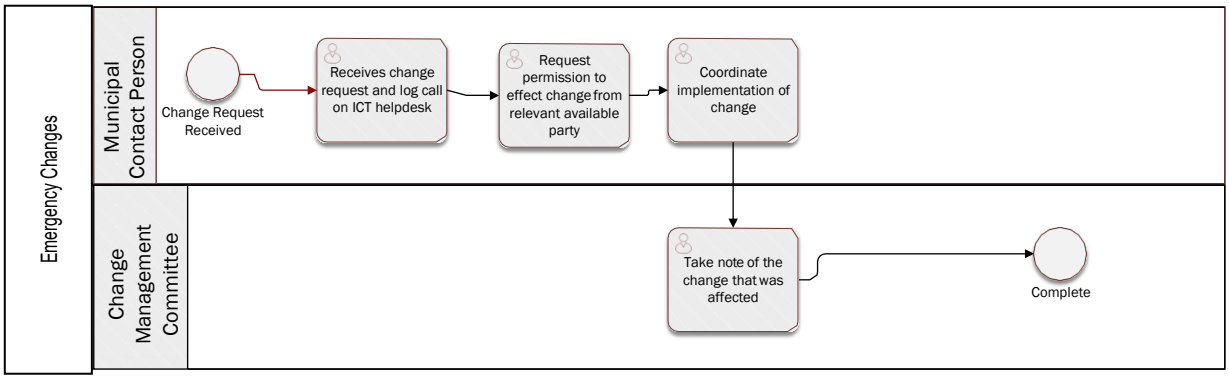
### 6.2.7. Emergency Changes

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 helpdesk@laingsburg.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 Laingsburg 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 service providers allowed. 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. CHANGE CONTROL (SECTION 22: SECURITY CONTROL POLICY)

7.4. All changes to Municipal applications and infrastructure must be managed in a controlled manner to ensure fast and reliable ICT service delivery to the Municipality, without impacting the stability and integrity of the changed environment.

a) Corrections, enhancements and new capabilities for applications and infrastructure will follow a structured change control process.

b) An emergency change must follow a structured change control process, but with the understanding that documentation must be completed afterwards. Emergency changes are only reserved for fixing errors in the production environment that cannot wait for more than 48 hours.

c) Recurring change requests from users (e.g. user access requests, a password reset, an installation, move or change of hardware and software etc.) must follow the processes designed to deliver ICT services in the most effective way.

d) Recurring operational tasks are excluded from the structured change control process.

7.5. The following additional rules with respect to change control must be adhered to. In some cases this may not be cost-effective or technically possible, in which case it is the duty of the ICT Manager to review and approve alternative controls:

a) The same person who performs the change may not implement the change.

b) Systems must have a development environment where testing is conducted to avoid testing in the production environment.

c) If a vendor performs the change, the Municipality must also test the change.

d) The data inside a database may not be edited, except through an approved application front-end. This excludes internal system processes or interfaces, or work required to convert data during a system implementation.

e) Commercial software must be selected after considering information security requirements.

f) The affected user's willingness to change must always be considered when documenting all that can go wrong with the change.

g) Any system published to the Internet or on a mobile platform must reviewed by security specialists before being deployed

7.6. The ICT Manager must record all change requests across the Municipality in a central tool, file server or spreadsheet. This implies that changes performed by ICT and those changes requested by the business from vendors, without ICT involvement, must be recorded together.

7.7. The ICT Manager must create a weekly report which lists all of the unapproved change requests, active changes requests, cancelled change requests and completed change requests. The report must be reviewed, and actions taken, to ensure that

- Change requests receive sufficient attention;
- The change control process is being followed for all known changes; and
- Trends across change requests, that indicate systemic problems in the ICT environment, are identified and require more permanent fixes.

## 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. Regression / Role-Back Testing

In the event that the changes implemented into the Production Environment is not operating correctly, either causing failures or is producing incorrect results, compromising business and system deficiencies:

a) Explain the reasons to the CMC and get their approval to roll-back changes.
b) Identify all the changes that has been rolled out to production
c) Liaise with Vendors; if necessary, to regress to the previous versions of the system.
d) After roll-back, re-testing must be performed to ensure that all systems have been restored to its original state before the changes were implemented into the ‘Live’ or production environment.

### 8.4. Change register

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

## 9. CONTROLS

The following controls apply:

- 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 there to, 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.

## 12. CHANGE (SECTION 9: ACCESS MANAGEMENT POLICY

### 12.1. New User Registration

a) A formalised user registration process must be implemented and followed in order to assign access rights.

b) All user access requests must be formally documented, along with the access requirements, and approved by authorised personal by making use of the user access request form. The template for this type of request can be found attached to the Access Management policy in Annexure B.

c) User access requests must be obtained from the ICT department on registration of a new employee. The form must be sent to the service provider/line manager for access requirements to be requested. Once the requirements have been requested and signed off by the departmental manager, the form must be sent to the ICT department for approval following which the activation of the employee based on the specified requirements will be completed and stored for record keeping purposes. Records of user access granted must be stored for a minimum of 10 years.

d) User access must only be granted once approval has been obtained.

e) All users must be assigned unique user IDs in order to ensure accountability for actions performed. Should share accounts be required to fulfil a business function, this account must be approved and documented by the Risk Management Committee.

f) The diagram below depicts the formal new user registration process to be followed:

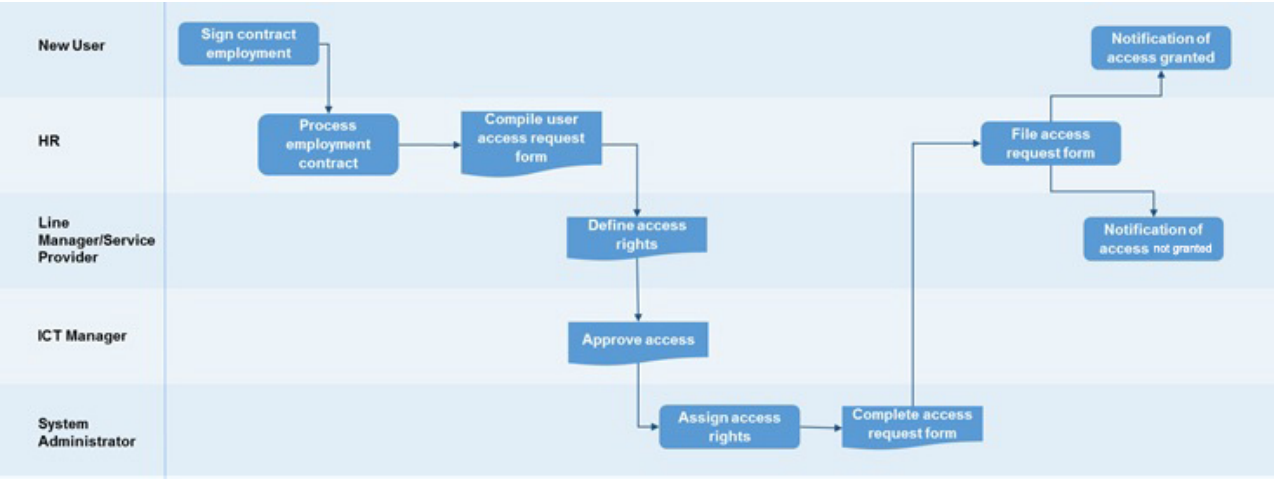



**Figure 1: New user registration process**

## 13. CHANGE (SECTION 10: ACCESS MANAGEMENT POLICY)

### 13.1. Terminated User Removal

a) A formalised user termination process must be implemented and followed in order to revoke access rights.

b) All user termination requests must be formally documented and approved by duly authorised personnel. Access must be disabled immediately, with accounts being removed after 6 months once authorisation has been obtained by line manager.

c) Terminated user requests must be obtained from the ICT department on the termination of an employee. The template for this type of request can be found attached to this Access Management policy in Annexure B. The form must be sent to the service provider/line manager for access revocation to be signed off. Once access revocation has been signed off, the form must be sent to the ICT department for approval and deactivation of employee based on specified requirements and stored for record keeping purposes. Records of user access removal must be stored for a minimum of 10 years.

d) The diagram below depicts the formal user termination process to be followed.

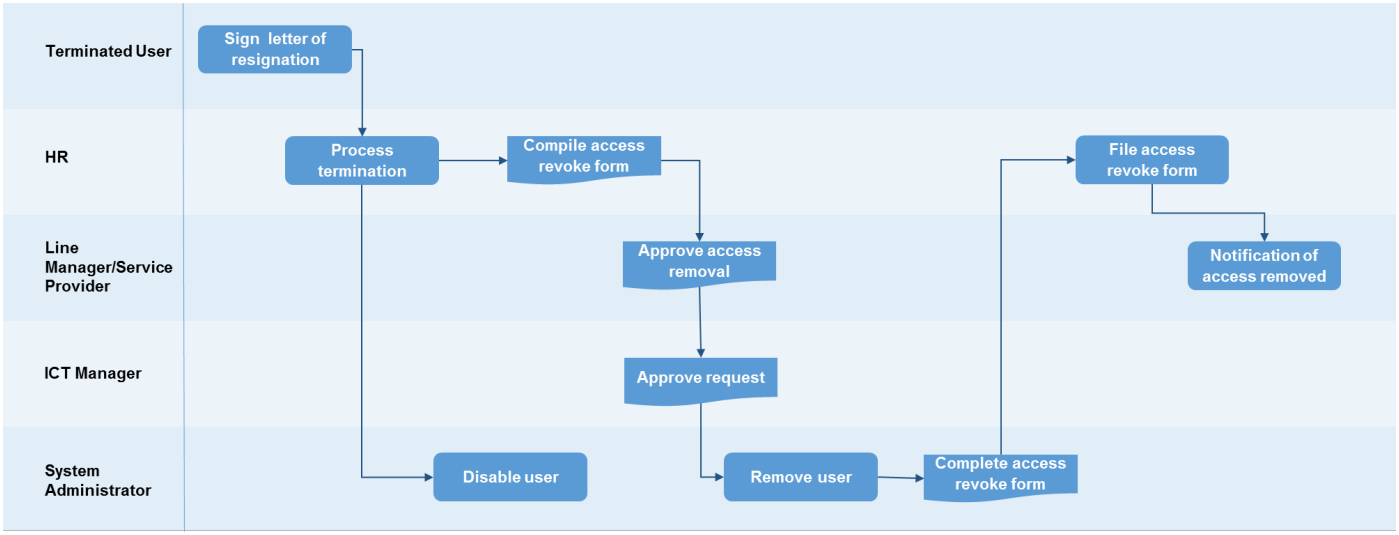



**Figure 2: User termination process**

## 14. CHANGE (SECTION 10: ACCESS MANAGEMENT POLICY)

### 14.1. User Permission/Role Change Request

a) A formalised user access management process must be implemented and followed in order to adjust user access rights.

b) All user access change requests must be formally documented, along with their access requirements, and approved by duly authorised personnel.

c) Access must only be granted once approval has been obtained by the respective line manager.

d) User access change requests must be obtained from the ICT department on change of an employee's role or permissions. The template for this type of request can be found attached to this policy in Annexure B. The form must be sent to the service provider/line manager for access requirements to be signed off. Once the access requirements have been signed off, the form must then be sent to the ICT department for approval and adjustment of employee's access rights based on specified requirements and stored for record keeping purposes. Records of user access granted and removed must be stored for a minimum of 10 years.

e) User access rights that are no longer required must be removed immediately.

f) The diagram below depicts the formal user permission/role change request process to be followed.

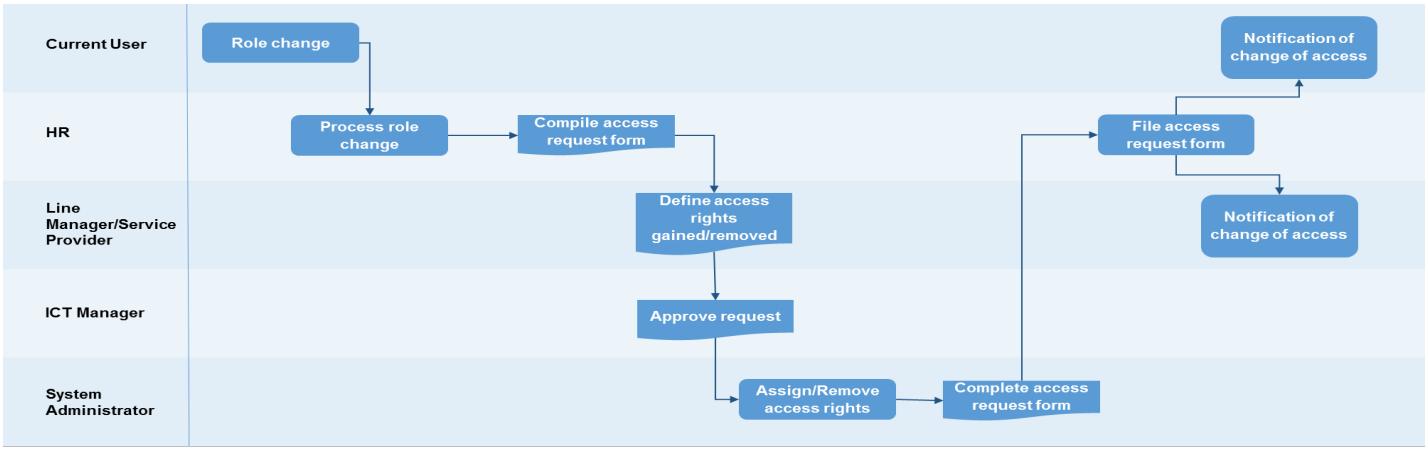



**Figure 3: User permission/role change request process**

## 15. ANNEXURE A: CHANGE MANAGEMENT FORM EXAMPLE:

| | | | |
|---|---|---|---|
| **To:** | **Documenting all changes made in the ICT environment** | | |
| **Copies:** | Senior Manager: Finance and Corporate Services | **Enquiries:** | Realdo Pedro |
| **Reference #:** | 1020200602 | **Date:** | 2020/06/17 |
| **Subject:** | **REFERING TO THE ICT CHANGE MANAGEMENT POLICY THAT GIVES AN INDICATION OF CHANGES THAT ARE MADE ALL RELATED ICT SYSTEMS, RESOURCES AND NETWORKS THAT IS USED BY LAINGSBURG MUNICIPALITY.** | | |

**1. Purpose of the ICT Change Management Policy:**

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

**2. The Scope of the ICT Change Management Policy:**

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 Laingsburg domain and/or applications and information systems and related infrastructure owned by or contracted for the use of the municipality.

**3. The Policy covers the following elements of user access management:**

3.1. Changes to ICT resources

3.2. Application for and Approval of Change Request

3.3. Changes to ICT Networks.

3.4. Changes to ICT Systems.

3.5. Change Control regarding the (Security Control Policy)

3.6. Change Management (Access Management Policy)

**Change Request Information:**

| | | | |
|---|---|---|---|
| **This change was requested by:**<br><br>_____<br>**ICT ADMINISTRATOR** | | | |
| **Change Description:** | | | |
| **Requested by:** | | **Personnel #:** | |
| **Designation:** | | | |
| **ID Number:** | | **Signed:** | |
| **Date:** | | | |

| Change Impact Evaluation | | | | |
|---|---|---|---|---|
| **Change Type** | | Application | | Database |
| | | Hardware | | Procedures |
| | | Network | | Security |
| | | Operating Systems/Utility | | Schedule Outage |

| | | | | | |
|---|---|---|---|---|---|
| **Change Priority** | | High | **Change Impact** | | Minor |
| | | Medium | | | Medium |
| | | Low | | | Major |
| **Change Request Description** | | | | | |
| **Change Approval or Rejection** | | | | | |
| **Change Request Status** | | Accepted | | | Rejected |
| **Change Scheduled for (Date):** | | | | | |
| **Representative (Optional)** | Name: | | Signature | | |

_____ _____

**SENIOR MANAGER FINANCE AND CORPORATE SERVICES** **DATE**