OVERBERG

DISTRICT MUNICIPALITY

ICT USER ACCESS MANAGEMENT POLICY

Council Resolution No:	.....
Date:	.....
Municipal Manager:	.....
Executive Mayor	.....
Reference No:	.....
Municipal Code No:	.....

Table of Contents

Glossary of Abbreviations

Abbreviation	Definition
COBIT	Control Objectives for Information and Related Technology
HR	Human Resources
ICT	Information and Communication Technology
ID	Identifier
ISO	International Organization for Standardisation
ODBC	Open Database Connectivity
PIN	Personal Identification Number
RAS	Remote Access Service
APN	Access Point Name
VPN	Virtual Private Network

Glossary of Terminologies

Terminology	Definition
Administrative rights	Access rights that allow a user to perform high level/administrative tasks on a device/application such as adding users, deleting log files, deleting users.
Bring Your Own Device	The practice of allowing employees to use their own devices, such as cell phones, tablets, laptops, or other devices for work purposes.
Business case	A formal requirement in order for a specific business function to perform its required task.
Clear text	Clear text refers to a message that has not been encrypted in anyway and can be intercepted and read by anyone.
COBIT	A best practice framework created by ISACA for Information Technology Processes and Controls for Governance of ICT.
Domain Administrators	Any natural person that has administrative access to the municipal domain.
Inactive account	A user account that has not been accessed or used for 60 days or more.
Line manager	Each department (HR, Finance, ICT, etc.) should have a manager employed to perform managerial tasks.

Terminology	Definition
Personal Identification Number	A number allocated to an individual and used to validate electronic transactions.
Principle of least privilege	A user or a program must be able to access only the information and resources that are necessary for its legitimate purpose.
Remote Access Service	A service which allows for a user to connect to a remote machine from any network point, as long as the targeted device resides on the network.
Segregation of duties	The principle of dividing a task up based on varying levels of authority in order to prevent fraud and error by requiring more than one person to complete a task.
System Administrator	Any natural person that has administrative access to an information system.
VPN	A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organisation's network.
Wi-Fi	Wi-Fi is a wireless networking technology that allows computers and other devices to communicate over a wireless signal.

1. INTRODUCTION

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 the processes. 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 to ensure that the ICT enabled business processes not to be interrupted or compromised in any way. This policy sets measures in place to ensure that people, process, and information are protected against possible risks.

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

- Exploitation of information systems by internal staff and external entities.
- Protect information against information system access related exploitation.
- Protect against the compromising of the integrity of ICT enabled business processes.
- Exploitation of information carried within automated processes; and
- Exploitation of personnel to gain access to business related information.

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

Administrator	An administrator is afforded full root level access to an information system or related domains. Administrators has the ability to use all functions available within a system and allocate users the necessary access and related rights according to their roles.
Application System	See information system.
ODM Domain	The computer identity of the Overberg District Municipality.
ICT Infrastructure	The necessary cabling, radio-links, servers, storage, user computer and back-up equipment used to enable information systems and applications.
Information System	An information system is used by users to electronically execute their duties.
User	An employee that makes use of municipal ICT infrastructure and information systems in the execution of their duties.

4. SCOPE

This policy applies to all staff and line function departments, ICT related service providers, ICT department and users of electronic information resources.

It addresses computer user identity management that have access to 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 ODM 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 ensure that only approved users be granted access to the domain and information systems with the correct access rights.

6. POLICY CONTENT

6.1. POLICY CONTEXT

Electronically stored information, as a resource, is playing an increasingly important role in the administration and service delivery of the municipality. It is important that the necessary means and mechanisms be put in place to ensure that:

- Electronic information within ICT systems and infrastructure be protected against unlawful user and server management, information system administrator access and exploitation.
- User access to ICT systems and infrastructure be granted to natural persons only and according to prescriptive segregated usage.
- Server administrator access to ICT systems and infrastructure be granted to natural persons only and according to the roles allocated to them by information system owners.
- User classification be performed by information system owners and allocated by the relevant administrator(s) to ensure that the right level of access to electronic information within the ODM domain, supporting back-end and application systems are granted.
- The access rights of administrators and users are granted according to approved access on the ODM domain, supporting back-end, information system and application level.
- Redundant user management is implemented; and
- User identity be managed.

6.2. OWNERSHIP OF INFORMATION SYSTEMS

Electronically stored information invariably belongs to the relevant line and staff function. Information systems are created to automate the line and staff function processes used to deliver services. These information systems are thus developed and implemented by the office of the Head ICT under the leadership with line and staff functions. These line and staff function are the owners of these information systems. Line and staff functions are ultimately responsible to define the administrator and user (employee with access to the electronically stored information and its related information systems) access required in accordance with the role of each employee.

6.3. SEGREGATION OF DUTIES

The allocation of information system and application administrator and user access rights according to their roles within the line and staff function is often informed by the regulatory and prescriptive landscape. This is so especially in supporting back-end (server operating systems and database management systems) and information/application systems that manage human resource and financial information/data and to a lesser degree in other environments.

The definition of administrator and user roles and allocation of access rights informed by the segregation of duties are directly influenced by the operational requirements of the relevant line and staff function processes. It is reflected within the information system via assigning administrator and user access rights.

Segregation of duties is however not limited to the staff and line function of the municipality. The office of the Head ICT inherently provides and administrates the supporting domain and back-end information and application systems that manage electronically stored information. Thus within the office of the Head ICT segregation of duties according to roles and responsibilities also applies system administrators.

User access management is applied according to the model described in the following paragraph.

6.4. USER ACCESS MANAGEMENT MODEL

The design and provisioning of user access thus falls within the domain of staff and line function and Head ICT. It is classified according to the following model.

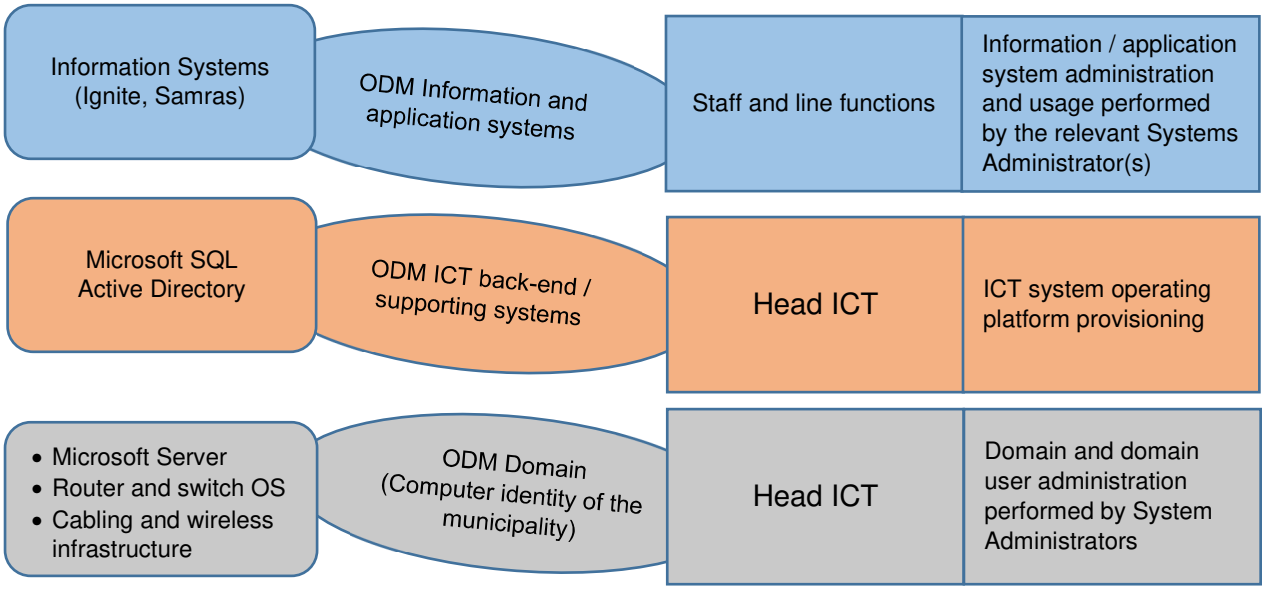


Diagram 1. ICT and Information System Administration and User Access Management Model

User access is classified as follows:

- **Domain user access –** all users of information systems are primarily provided access to the ODM domain. This level of access is initiated by the Human Resource Department and allocated by the relevant System Administrator(s).
- **Backend supporting systems and domain administrator access –** implies the management of access provided to the domain and related servers, applications, databases and other enabling infrastructure systems and their administrators, developers and operators that reside in the system administrator and service providers.
- **Information and application System Administrator and user access –** addresses the provisioning of access to information systems by the information system or application owner and allocated by the information system and application administrator (staff and line function management) according to the relevant role and segregation of duty requirements.

It is thus evident that the responsibility for user access management lies within various line and staff functions within the municipality. This policy provides guidance and parameters within which user access management must be administrated.

6.5. POLICY STATEMENTS

The following policy statements apply to: - staff, line, Human Resource and the ICT department must:

- Ensure that access to the ODM domain, supporting back-end information and application systems is only granted to approved natural persons (an exception is grated for direct system-to-system access).
- Approve and implement user access rights to the domain, supporting back-end, information systems and application systems according to regulatory and prescriptive requirements.
- Manage user identity, access and rights in line with regulatory and prescriptive requirements.
- Implement an access management practice to maintain and monitor access management through approved administrator and user creation, authentication and allocation of correct segregated administrator and user rights; and
- Monitor access and allocation of user rights according to the management practice.

Annexure A donates the areas of access management and its rules, processes, and controls.

6.6. DELEGATIONS

The following delegations apply in relation to this policy:

6.6.1. ODM domain access management:

- The definition of domain access to natural persons must be initiated by the Human Resource Department;
- Employee line managers define the type of domain access required; and
- Domain access is implemented by the ICT department.

6.6.2. Supporting back-end systems administrator access management:

- Approved and managed by the System Administrator; and
- Access is implemented by the ICT department or relevant System Administrator

6.6.3. Application system access management:

- Managed by the relevant staff and line function application system owners; and
- Implemented by information and application system administrators in the staff and line function.

6.7. MONITORING OF USER ACCESS

All information systems and Overberg District Municipality employees who have access to Samras, IGNITE and/or the ODM network will be reviewed on a quarterly basis. The ICT Department will send a list of employees and their access to the managers. The managers will make the required changes, if any, and send it back to ICT using the automated macros provided on the list mentioned above.

User access, including vendor user access, will be reviewed electronically on a quarterly basis. Any removal of access will be done based on the review. Any additional access required must be done by applying on the ICT User Access Application Form.

7. 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.

8. ADMINISTRATION

The System Administrator function is responsible for the administration of this Policy. This policy will be revised at least on a 3-yearly basis.

9. ANNEXURES

9.1. ADMINISTRATOR AND USER ACCESS RULES, PROCESSES AND CONTROLS

The user access rules, processes and controls are to be implemented by the relevant staff, line managers and HODs. ICT functions are discussed in the following paragraphs:

A. CLASS 1 USER

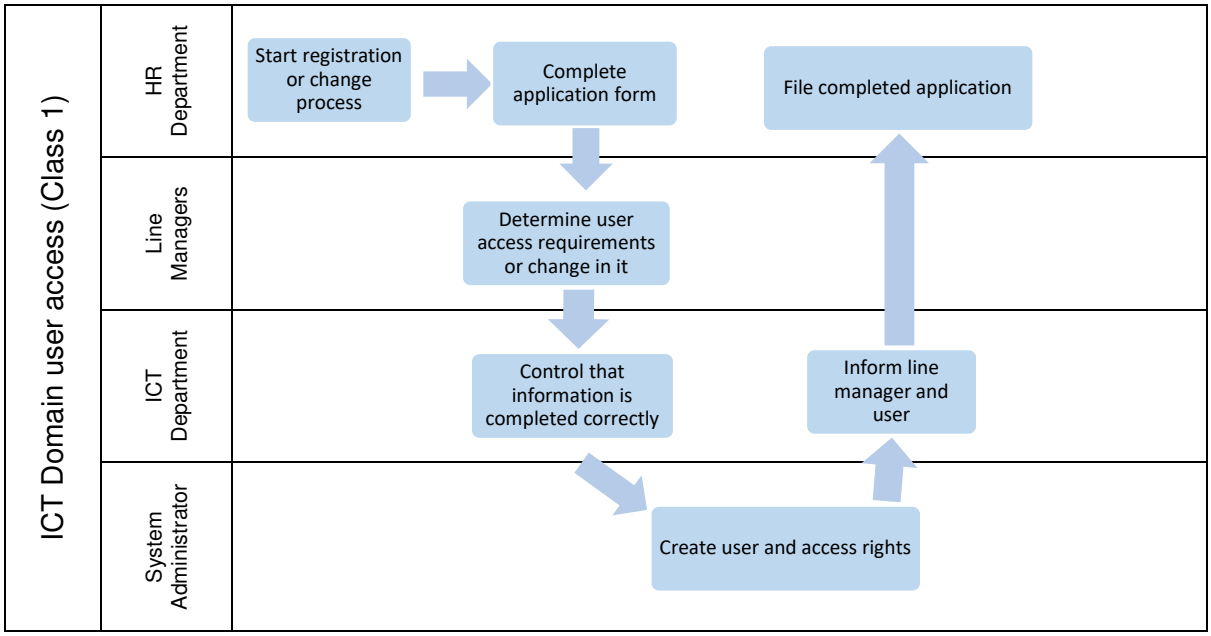
Approval of access to or change in access to the ODM domain and application services (Class 1 user)

- **Rules**

a. Human Resources Department are to inform the ICT department via a user access request form of new employees that requires access to the domain or whose change in employment influences their allocated user rights; and
b. User access rights are determined by the relevant staff or line function management.

- **Process**

a. The following process applies:



- **Control**

a. Completed user access or change request form;
b. Sign-off from System Administrator that user was created.

B. CLASS 2 USER

Approval of access to the supporting back-end information systems (Class 2 user)

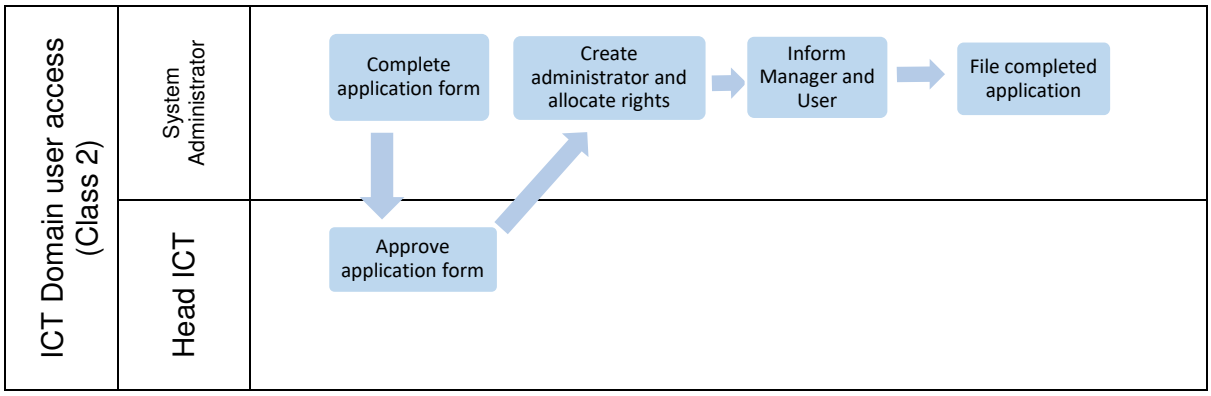
- **Rules**

a. The System Administrator determines administrative access of ICT employees and contractors that require access to supporting back-end information systems.

b. Only domain users can be granted administrator access to supporting back-end information systems.

- **Process**

a. The following process applies:



- **Control**

a. Completed and approved application form;

b. Sign-off from by the Head ICT that user was created.

10. DOMAIN, BACK-END & APPLICATION USER ID & RIGHTS MANAGEMENT

In the context of administration and user access to the Overberg District Municipal domain management it is necessary to confirm from time to time that all users are natural persons. Furthermore, it is also necessary to change the access rights of users as their roles change. This applies to all three areas of access: a) domain, b) supporting back-end, and c) line and staff function application systems. In this regard the following processes and controls apply:

10.1. MANAGE USER IDENTITY

- **Rules**

a. A six-monthly confirmation must be done to ensure that users are approved natural persons with an identifiable username; (Refer to Sec 6.6 of this policy)

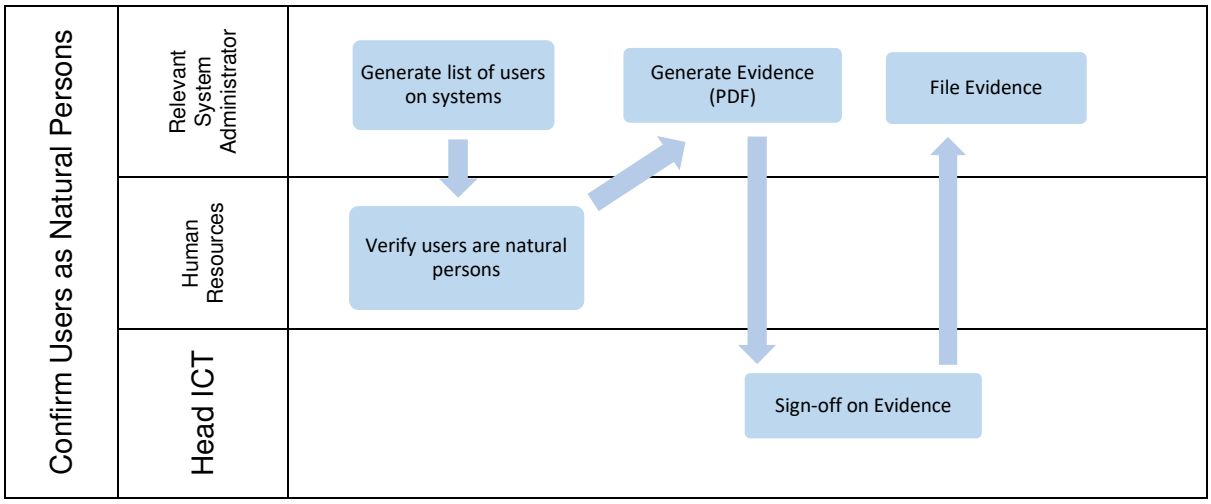
b. User access passwords can only be reset on identification of the user or where a temporary password is sent to the user e-mail address or communicated via phone; and/or

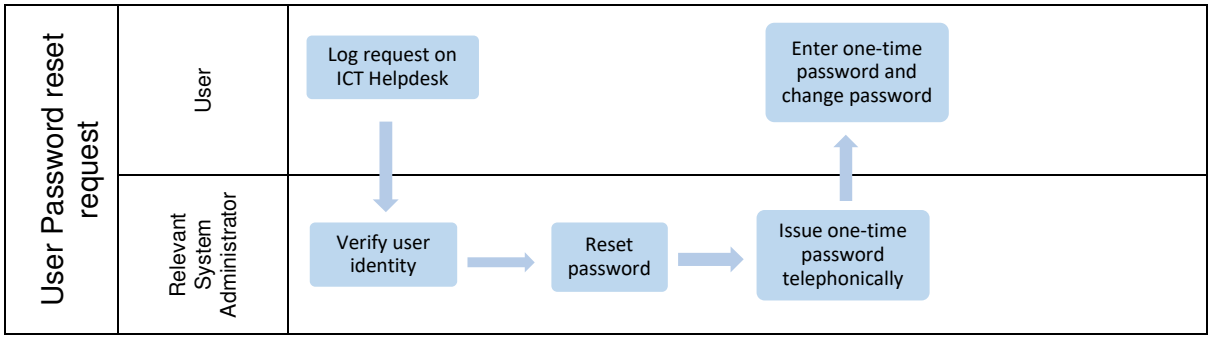
c. Alternative identification mechanisms should be implemented where the user, for instance, have to click a link to reset the password or receive a verification notification via a short message service or secondary e-mail address.

d. Under no circumstances may a user give out any password to another user. Should a user require a work-related document or email from another user and said user can't provide it (user is on leave), then written (email) permission must be obtained from the relevant Senior Manager, Director or the Municipal Manager. The System Administrator will then log into the relevant computer and provide the document or email to the requesting user.

- **Process**

a. The following processes apply:





- **Control**

a. Proof of six-monthly confirmation of user being a natural person by Human Resources Department.
b. Domain password change requests recorded on the helpdesk; and
c. Where applicable (non-Active Directory linked application and information systems) password change requests are managed by the System Administrator.

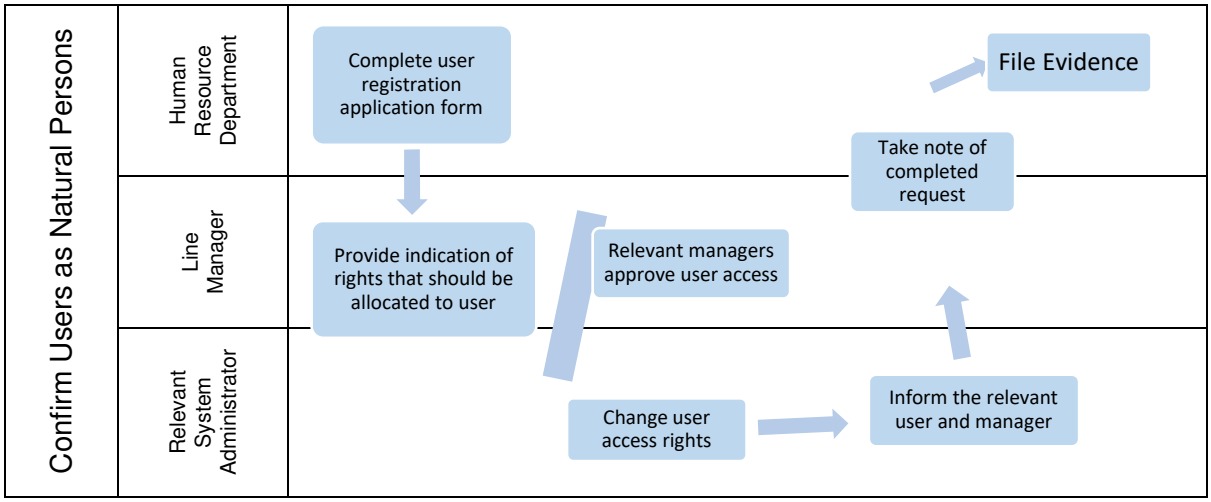
10.2. MANAGE CHANGE IN USER ACCESS ROLES AND RIGHTS

- **Rules**

a. User access rights to the domain, application and information system may only be assigned according to the individual role and rules within the segregation of duties; and
b. Only approved changes to user access rights may be affected.

- **Process**

a. The following processes apply:



- **Control**

a. Completed change request form.

10.3. USER ACCOUNT LOCK OR REMOVAL

- **Rules**

a. User accounts of employees that leaves the municipality will be locked on notification from the Human Resource Department.

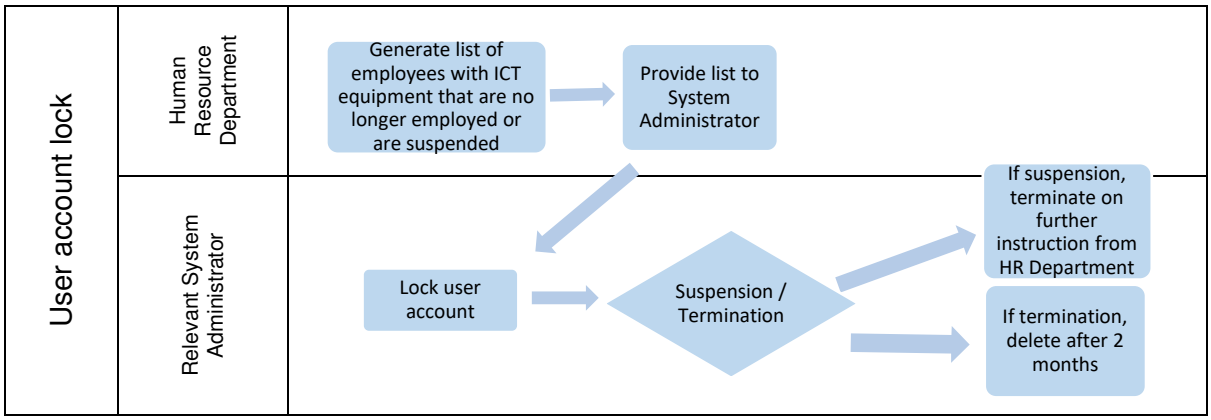
b. User accounts will be deleted 2 months after it was locked on the original instruction from the Human Resource Department.

c. The user accounts of suspended employees of the municipality will be locked and only deleted on instruction of the Human Resources Department; and

d. User accounts may be locked on an emergency request approved (via e-mail) by the Senior Manager Corporate Services or the Head ICT.

- **Process**

a. The following process applies:



- **Controls**

a. Completed access revoke or account delete instruction from HR.

10.4. USER ACCOUNT MANAGEMENT

- **Rules:**

a. User password policy

- Minimum password length = 8 characters.
- Maximum password age = 30 days.
- Password history retention = 12.
- Password complexity enabled.

b. Server farm manager and administrator password policy

- Minimum password length = 12 characters.
- Maximum password age = 30 days.
- Password history retention = 12.
- Password complexity enabled.

c. User accounts must conform to the following account lockout configurations:

- Account lockout duration of 60 minutes or more.
- Account lockout threshold of 5 attempts or less.
- Account lockout counter must be reset after 15 minutes.

d. Accounts with server farm manager and administrative access rights must conform to the following account lockout configuration:

- Account lockout duration of 60 minutes or more.
- Account lockout threshold of 5 attempts or less.
- Account lockout counter must be reset after 15 minutes.

- **Controls**

a. User accounts can only be allocated to approved natural persons;
b. Printout used account network settings;

c. The System Administrator will review all related network settings on a quarterly basis; and
d. The Head ICT will review all related network settings on an annual basis.