CHRIS HANI
DISTRICT MUNICIPALITY
SUSTAINING GROWTH
THROUGH OUR PEOPLE

USER ACCOUNT MANAGEMENT POLICY

Active Directory

REFERENCE NUMBER	**6/1/2/7/P/012**
SECTION RESPONSIBLE FOR FORMULATION	**ICT Section**
EFFECTIVE DATE	**01 July 2024**
POLICY PUBLISHED DATE	**01 July 2024**
DATE OF NEXT REVIEW	**June 2025**

Adopted in an Ordinary Council meeting held on 24 May 2024

Approval

DOCUMENT:	**User Account Management Policy – Active Directory**		
Copy Number:	**Original Copy**		
Compiled by:	Lamla Luke	**Reviewed by:**	Management and Council
Compilation Date:	April 2021	**Review Date: Management**	
Version:	V 1.0	**Review date: Council**	
Distribution:	All	**Classification:**	**Policy**
Document Release		**Document Approval**	
Releasing Authority:	Director: Corporate Services	**Approval Authority:**	CHDM Council
Date Released:		**Date Approved:**	**24 May 2024**

Contents

1. Problem Statement

ICT user accounts are one of the primary mechanisms that protect potentially sensitive municipal network and information resources from unauthorized use. While accounts administration and monitoring are not the most secured way of protecting information and information systems, constructing secure ICT user accounts, and ensuring proper password management is essential. Poor ICT user account management and protection can allow both the dissemination of information to undesirable parties and unauthorized access to departmental network resources.

2. Purpose

The purpose of this policy is to establish a standard for the administration of IT systems accounts that facilitate access to Chris Hani District Municipality IT Environment.

3. Scope

This policy is applicable to all users and third parties authorized under CHDM to have access to any of the CHDM IT systems.

4. Legislative References

- Minimum Information Security Standards
- International Standard for Risk Assessment
- Electronic and Communications Act, 2002 (Act 68 of 2002).
- Protection of Personal Information Act
- ISO 27001- information security management,
- Information Technology Infrastructure Library (ITIL) and

- King IV on corporate governance

5. User Account Creation

a) User access requests must be obtained from HR on registration of a new employee. The form must be sent to the line manager for user access requirements to be authorized by the line manager. Once the requirements have been requested and signed off by the departmental manager, the form must be sent to the ICT unit for approval following which the activation of the employee based on the specified requirements will be completed. The form must then be sent back to HR for record keeping purposes.
b) The identity of users shall be authenticated before providing them with account and password details.
c) Passwords for new accounts must **NOT** be emailed to users.
d) The date when the account was issued shall be recorded in an audit log.
e) When establishing accounts, standard security principles of "least required access" to perform a function shall always be used, where administratively feasible.
f) A root or administrative privileged account must not be used when a non-privileged account will do.

6. Modifications/Changes

Changes in user status include changes of job function, roles, responsibilities, and transfers within the Municipality. A procedure should be established to manage these changes in user status.

7. User De-registration

All user termination requests must be formally documented and approved by duly

authorised personnel. Upon receiving necessary HR documentation, account must be disabled immediately then account will be removed according to records management policy and file plan of the municipality.

8. Review of User Access

a) Accounts shall be reviewed at least quarterly by IT staff to ensure that access and account privileges are corresponding with job function, need-to-know, and employment status. The IT staff may also conduct periodic reviews for any system connected to the Chris Hani District Municipality IT environment.

b) All third-party accounts of the Chris Hani District Municipality with access to Chris Hani District Municipality IT environment shall contain an expiration date of one year or the work completion date, whichever occurs first.

9. User Responsibilities

The cooperation of authorised users is essential for effective security. Users should be made aware of their responsibilities for making effective access controls particularly regarding the use of passwords.

10. User password management

a) The user password management must adhere to CHDM password management policy.

11. Monitoring of access user activities

a) Users and administrators activities must be monitored through audit and event

logging on a monthly basis.

b) Once a month, network administrators must review audit and event logs for suspicious and malicious activities.

c) Dormant accounts should be disabled.

d) All reviews must be formally documented and signed off by the IT Management. Documentation must be kept for record keeping purposes.

12. Audience and Applicability

The user account management policy is applicable to everyone in the Municipality who has access to the active directory services and network infrastructure of the Municipality.

13. Responsibilities of the Municipal Manager

The Municipal Manager at the advice of the Manager ICT can decide on the following:

1. Review of the user account management policy,
2. Change the user account management policy if it is not compliant with information security legislation,
3. Propose amendments and and/or deletions on the guidelines.

14. Responsibilities of the IT Management

1. The IT Management is responsible for the assessing and evaluating of the risk on the accessing of the abuse or miss-use of affected computer systems.
2. Appropriate rights or revocation thereof of those rights to the Municipal employees violating the user account management policy,
3. Ensure that the user account management policy is effective and user friendly.
4. Must sign-off user account reviews

15. Escalation Procedure

1. The IT Staff shall escalate any deviations or violation of the user account management policy to the IT Management.
2. The IT Management shall immediately issue a directive to the IT Staff to suspend the use of certain devices to institute a formal and proper investigation.
3. On the outcome of the investigation, the IT Management shall inform the Municipal Manager of such for a ruling or further investigation upon which a decision shall be taken on the necessary course of action.
4. The Municipal Manager may allow deviation only based on an operation that requires such an intervention.
5. The Municipal Manager may approve or decline such request for a deviation.

16. Policy Compliance

Compliance Measurement

The IT Staff will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exceptions to this Policy must be approved in writing by the Municipal Manager.

Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. IT Staff reserves the right to restrict any device or connection that does not comply with this policy.

Reporting & Disclosure Requirements

The IT Management shall report from time to time the management, administration, and operationalisation of the policy implementation to the Municipal Council.

Review of this policy

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

Approval

EFFECTIVE DATE

The effective date of this policy, or any amendments thereto, shall be the date of its adoption by Council. This Policy takes effect on the **01st of July 2024.**

User Account Management Policy adopted on the Chris Hani District Municipality council meeting; dated **24 May 2024**

Council Resolution number: **C143**

2023-2024

Signed by Municipal Manager: G. Mashigi _____ _____

Initial & Surname *Signature* *Date*

Signed by Speaker of the Council: _____ _____ _____

Initial& Surname *Signature* *Date*