CHRIS HANI
DISTRICT MUNICIPALITY
SUSTAINING GROWTH
THROUGH OUR PEOPLE

CHRIS HANI DISRICT MUNICIPALITY

User Accounts Management Policy and Procedure

DEFINITIONS

CHDM	Chris Hani District Municipality
Computer	A computer is a device that accepts information (in the form of digitalized data) and manipulates it for some result based on a program or sequence of instructions on how the data is to be processed. Includes server, desktop computer, laptop computer, monitor, cables, mouse, keyboard, all software, cards, components and all other software that enhance performance of a Computer or any part or portion of the above mentioned.
HOD	Head Of Department
VPN	Virtual Private Network used to connect to the CHDM network using the internet
AD	Active Directory
SCM	Supply Chain Management
BTO	Budget and Treasury Office
CSD	Corporate Services Department
ICT	Information Communication Technology

1. BACKGROUND

ICT user accounts are one of the primary mechanisms that protect potentially sensitive departmental 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. LEGISLATIVE FRAMEWORK

Information Act of 2002
MFMA of 2003
King 3 Report

3. PURPOSE

This policy establishes standards for issuing accounts, creating password values, and managing accounts. An account, at minimum, consists of a user ID and a password; supplying account information will usually grant access to some set of services and resources.

The purpose of this policy is to:

3.1. Establish a standard for the creation of user accounts
3.2. Ensure proper access control
3.3. Ensure protection of passwords
3.4. Establish a minimum time between changes to passwords

4. THE SCOPE OF THIS POLICY

This policy is applicable to all users and to all systems (Financial and non-financial) of CHDM. This means all employees that are employed permanently, contracted or temporary, Councilors and service providers and consultants using Chris Hani District Municipality network and Application Systems. All these employees will be referred to as "users" in the rest of this document.

This policy is applicable to those responsible for the management of ICT network user accounts or access to shared information or network devices and all application systems of CHDM.

5. POLICY

REQUEST FOR USER ACCESS

1. A User Access Form which is available on the intranet/ICT office/Systems office must be filled indicating what access is required for which system and signed by the relevant section head.
2. For Active Directory all user accounts must be uniform i.e. initial & surname e.g. nsmith for Nomsa Smith. This username will apply to windows logon, email account (email address) and FNB online (banking system). (exception of cases where naming conversion is same in more than one person)
3. Network and Systems Administrators are responsible for defining access controls and levels.
4. Assistant Director: Systems and ICT Manager shall be informed new user access to the network and application systems.
5. All users to sign Acceptable Use Policy before their accounts are created.
6. All access to the following systems (Venus/ Solar, Payday, FNB online) must be reviewed quarterly.

7. All systems should enforce segregation of duties, i.e. one user captures, second one verifies and the last authorizes.
8. Systems and Network Administrator are responsible for performing user access reviews and review of audit logs on a quarterly basis.
9. User accounts shall be set to expire every six months on Active Directory and Password is set to expire monthly.
10. Assistant Director Systems and ICT Manager are responsible for performing reviews on Administrators' accounts.

5.1. VENUS / SOLAR

5.1.1. Everyone who is an employee of CHDM finance Department shall have a username for Venus/ Solar and given access to application according to his or her duties.

5.1.2. The username must be five characters starting with "ch" then the number cumulative on the system, linking the username and password to active directory (AD).

5.1.3. The users use same username that is created in Domain to access Venus/ Solar application.

5.1.4. There are different levels of access:

- Level 1 - For the CFO and top management at BTO
- Level 2 - For Senior Accountants and Accountants(Supervisors)
- Level 3 - For everyone else (implementers)

5.1.5. All other employees from other departments with CHDM will get a level 3 with view and print only.

5.1.6. Audit logs shall be reviewed on a quarterly basis, and when need arises

5.1.7. Super user account shall be reviewed annually by an independent

external body.

5.2. FNB ONLINE/ EFT PROCESS

5.2.1. Employees of CHDM who are the signatories at the bank will have the username with authorization functionality (access) only. Employees that work with Bank control or bank statements within the BTO can also have usernames accordingly with the duties they perform.

5.2.2. All computers must have internet access.

5.2.3. A user will be created and given a profile that will only be linked to the user's cellphone and the profile regardless of the desktop or laptop the user is working on to enhance security levels.

5.2.4. Two administrators are required for the purpose of access control on the system and the Assistant Director: Systems and systems administrator are responsible for this.

5.2.5. Two authorizers are required to authorize the payments that are imported from Venus/ Solar.

5.2.6. The accounting officer will appoint managers that will authorize and release payments. The users that have access to authorize can be more than two and may not necessarily be the signatories of the bank account.

5.2.7. One of the two users that are authorizing will check the vouchers, sign the payments list and be the first to authorize on the system.

5.2.8. In case where the checker is unable to connect for authorization, can request other authorisers to release payment **BUT** the checker **MUST** sign the vouchers to certify their correctness.

5.2.9. System Administration Office also has a responsibility to print and review the logs for any abnormalities monthly.

5.2.10. Two passwords will be allocated to the authorizing users, one for login to the system and the second one for authorization.

5.2.11. Audit trail is ran on FNB online as per the specific period one is looking and the information is always retained on the system.

5.2.12. User accounts are reviewed quarterly.

5.3. PAYDAY SYSTEM

5.3.1. Employees of CHDM who are working at BTO and CSD will be allocated user numbers and passwords that will give them access to the Payday System.

5.3.2. All access must be allocated according to the duties of the employee.

5.3.3. One user number and password will give the user access to all payday companies of CHDM.

5.3.4. It remains the responsibility of the employees not share their username and password.

5.3.5. Audit trails must be printed, reviewed and singed at least once per month by the Manager: Expenditure.

5.4. CASHDRAWER

5.4.1. Employees of CHDM that are working at the Income Section and managers involved in the Cash Management process will have a cashier number and a password to login to the system.

5.4.2. Access will be allocated accordingly with the duties that they perform.

5.4.3. There are different levels of access control

5.4.3.1. Cashier - For capturing

5.4.3.2. Supervisor - For balancing and cash-up

5.4.3.3. Manager - Reports and analysis

5.4.4. Cashiers may not cancel receipt or balance themselves without the authorization of the supervisor or a manager.

5.4.5. Managers may not capture any receipt. (segregation of duties applied)

5.4.6. It remains the responsibility of the employees not share their username and password.

5.5. **CASEWARE**

5.5.1. This is report writer software that is used to draw up financial reports, from different financial systems, e.g Annual financial statements, Sec 71 reports, monthly management accounts etc. All users that are using this system are given access by the system's administrator, according to their duties.

5.6. **ROUTEMASTER SYSTEM**

5.6.1 Read meters without manually capturing readings. You can utilize the rugged hand held computers to read your billing registers through an optical probe using the Flag protocol.

5.6.2 Once the meter has been read electronically the reading information will be transferred through to your RouteMaster Meter Reading System which in turn would transfer the relevant data to Billing System which is Solar for billing purposes.

6. DISABLING AND DELETING USER ACCOUNTS

6.1. When an employee leaves the employ of Chris Hani District Municipality, HR shall complete an Employee Termination Checklist Form and immediately send it to Assets management section, Credit Control section,

ICT and Systems and lastly Payroll office before the employ is released and all the monies are paid.

6.2. Upon receiving the form from HR, the account will be set to expire on the last day of work of the employee and the user account will be disabled by ICT from AD immediately and be deleted after six months and where applicable be disabled from Financial Systems accounts immediately by Systems Administration.

6.3. For Venus/ Solar Financial System the user account will not be deleted for a period of five years, in case later, there's information requested from that account. The username holds audit trails that may be needed at some stage.

6.4. HR shall send a list of terminated users to ICT and Systems Administration on a monthly basis.

6.5. Upon receiving the list, Network and Systems Administrators shall review user accounts accordingly.

6.6. Usernames and Passwords may not be shared by users, it is illegal and changes maybe be drawn against anyone who does not comply.

7. HOW THIS POLICY WILL BE APPLIED

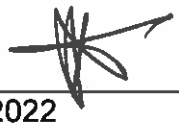
7.1. This policy will be applied automatically in systems that can allow automation else manually enforced.

7.2. The manager of the employee alleged to have violated this policy shall be responsible for ensuring that disciplinary proceedings are commenced with in terms of CHDM disciplinary procedure and policy. A failure on the part of such manager to take the necessary steps regarding disciplinary action

shall in itself be grounds for disciplinary action being instituted against the manager concerned.

7.3. Managers should ensure that all their personnel are made aware of the contents of this policy.

7.4. Managers are required to apply the policy to subordinates reporting to them.

Policy Particulars			
Signature by Municipal Manager:			
Signature by speaker of the Council:			
Commencement Date:		1 July 2022	
Revision History:		10 May 2021	
Review Date: 25 MAY 2022		Annually	
Policy Level:		All users of the Chris Hani District Municipality's computing facilities	
Responsibility - Implementation &Monitoring:		Assistant Director: Systems	
Reporting Structure:		Assistant Director: Systems » CFO » Municipal Manager » Council	
Version	Date	Author	Details
1st Version	August 2012	Assistant Director: Systems	
2nd version Final	Draft Review 04/06/2019	AD: Systems and IT Manager	
3rd Version Final	Review date 2022/02/14	AD: Systems and IT Manager	