



ICT User Access Management Policy

Date Approved	Version
	1

ICT Manager

Dr. Nkosazana-Dlamini Zuma Local municipality

Main Street

Creighton

Telephone(039) 833 1038

Facsimile (039) 833 1179

Website: www.ndz.gov.za

ICT User Access Management Policy

As a government institution, Dr Nkosazana Dlamini-Zuma Municipality must implement an ICT User Access Management Policy to maintain an adequate level of security to protect the Municipality's data and information systems from unauthorized access and to ensure a secure and reliable operation of the Municipality's information systems.

Full Title	Doctor Nkosazana Dlamini-Zuma Municipality Municipality's ICT User Access Management Policy
Short Title	ICT User Access Management Policy

Table Of Contents

1. Version Control	3
2. Definitions.....	4
3. Introduction	5
4. Objective	5
5. Scope/Audience	5
6. Policy	5
7. Policy Violations.....	9
8. Policy Review.....	10
9. Publishing the policy	10
10. Doctor Nkosazana Dlamini-Zuma Municipality Approval and Sign-Off	11

1. Version Control

Full Title	Doctor Nkosazana Dlamini-Zuma Municipality IT User Access Management Policy
Short Title	User Access Management Policy
Author(s)	0.1
Version	

Authors

Version	01
----------------	----

Authorized By	Council
---------------	---------

Authorization Date

Effective Date

2. Definitions

Term	Meaning
IT	<u>Information Technology</u>
ICT	Information and Commu
Municipality, the	Doctor Nkosazana Diam
CFO –	Chief Finance Officer
LAN –	Local Area Network
VPN	Virtual Private Network
SSH	Secure Shell
FTP –	<u>File Transfer Protocol</u>
DrNDZ –	Doctor <u>Nkosazana D</u>

3. Introduction

The main goal of Information Security is to protect the municipality's information resources from risks that affect the confidentiality, integrity and availability of the information. logical access to the municipality's information assets needs to be managed in a controlled manner and logical access permissions granted on the basis of business requirements. lack of adequate logical access controls could lead to unauthorized access to information and information assets.

4. Objective

The objective of this policy is to ensure the effective and efficient management of access to the municipality's information resources and systems and includes:

- Granting access after relevant management authorization and an official request has been received.
- Removing access upon role change, service termination or contract expiry.
- Resetting of access on positive identification of the owner of the user ID as the requestor.
Updating access as required after an official authorized request has been received.
- Regularly reviewing the granted access privileges of users to determine whether they are still valid and necessary.

5. Scope/Audience

This policy applies to all employees of Doctor Nkosazana Dlamini-Zuma Municipality and all contractors, consultants, temporary employees and business partners.

6. Policy

6.1 Authorized Users

6.1.1 Only authorized users are granted access to information systems and users are limited to specific defined, documented and approved applications and levels of access rights.

6.1.2 Computer and communication system access control is to be achieved via user IDs that are unique to each individual user to provide individual accountability.

6.2 Authentication

6.2.1 Any User (remote or internal), accessing, Doctor Nkosazana Dlamini-Zuma Municipality networks and systems must be authenticated.

6.2.2 Entity authentication includes but is not limited to:

6.2.2.1 A unique user identifier

6.2.2.2 A password

6.3 Disclosure Notice

6.3.1 A notice warning must be displayed before a user signs on to the system. The warning must stipulate that only authorized individuals should access the system.

6.3.2 The warning message must clarify that the system is a private network or application and unauthorized users should disconnect or log off immediately.

6.4 Access Approval

6.4.1 System access or modification to access will not be granted to any user without appropriate approval first.

6.4.2 Management is to immediately notify and report all significant changes in end-user duties or employment status to the IT Manager. The IT Manager should also be informed as to how access rights on systems should be updated due to role changes.

6.4.3 User access is to be immediately revoked or disabled if the individual's employment has been terminated. In addition, user privileges are to be appropriately changed if the user is transferred to a different job role.

6.5 Limiting User Access

6.5.1 Access to applications and systems will be granted based on a user's business requirements.

6.6 Access Privilege

6.6.1 Users will be granted access to information on a least privilege basis. That is, users will only receive access to the minimum applications and privileges required for performing their relevant jobs.

6.7 Compliance

6.7.1 Users who access, Doctor Nkosazana Dlamini-Zuma Municipality's information systems must sign a compliance statement prior to issuance of a user ID. Refer to the Dr NDZ Municipality's ICT Security Policy for further details.

6.7.2 A signature on this compliance statement indicates the user understands and agrees to abide by Dr NDZ Municipality's policies and procedures related to computers and information systems.

6.7.3 Annual confirmations will be required of all system users.

6.8 Registration of new users

6.8.1 The ICT Manager must be notified by Human Resources (HR) to create a new user account.

6.8.2 A User Access form must be completed and approved by the user's line manager.

6.8.3 Access will be granted by the ICT Manager upon receipt of the approved User Access Request form.

6.9 Resetting a Password

6.9.1 All password reset requests must be submitted by completing a User Access Form.

6.9.2 The user access form should be submitted to the IT department for approval and processing.

6.9.3 A change of password is forced on the first logon with the reset password.

6.10 Privileged/ Super User Access

6.10.1 For security reasons Dr NDZ Municipality must limit the number of super users in the municipality only to individuals who have a justifiable business use for such access.

6.10.2 An approval process for granting and requesting super user access must be followed.

6.11 System Access Controls

6.11.1 Access controls will be applied to all computer-resident information based on its Data Classification (refer to the ICT Security Policy) to ensure that it is not improperly disclosed, modified, deleted or rendered unavailable.

6.12 Access for Non-employees

- 6.12.1 Individuals who are not employees, contractors, consultants or business partners must not be granted a User ID or otherwise be given privileges to use Dr NDZ Municipality Municipality's computers or information systems unless the written approval of the relevant Director has first been obtained and then sent to and approved by the ICT Manager and CFO.

6.13 Remote Access

- 6.13.1 Any computing device used remotely must be updated with the most recent security patches.
- 6.13.2 All machines on the Dr NDZ Municipality's LAN as well as any remote computing device must run the most up-to-date versions of antivirus software with regularly updated virus definitions, i.e. at a minimum, once a day. However, whenever deemed necessary by the ICT Manager, these updates may be required to run more frequently due to business requirements.
- 6.13.3 Any authorized user using a remote computing device outside the firewall must use the VPN to send and receive Dr NDZ Municipality's email or to access the Internet and Intranet accordingly. No Dr NDZ Municipality email may be sent using third-party email services (including, but not limited to, Gmail, Hotmail, Webmail, etc.).
- 6.13.4 Any authorized user accessing any computer or device on the LAN for remote management or administration must use SSH and/or VPN. For remote file transfer, employees must use VPN. Under no circumstances shall Telnet, FTP or any other unencrypted access methods be used.
- 6.13.5 All employees using any computing device to remotely access and connect to Dr NDZ Municipality's LAN shall not do so while still connected to any other network.
- 6.13.6 All employees requiring remote access to Dr NDZ Municipality's LAN must obtain approval from the ICT Manager.

6.14 Termination procedures

- 6.14.1 HR must notify the ICT Manager prior to the termination of an employee's employment to ensure that access is revoked on the employees last working day.
- 6.14.2 The terminated employee's user account must be disabled.

6.15 Audit Trails and Logging

6.15.1 Logging and auditing trails must be reviewed by the IT Manager.

6.16 Periodic Review of User Profiles and Access Rights

6.16.1 A review of all user accounts must be performed on an annual basis by the appropriate business unit managers in conjunction with the ICT Manager.

6.17 Workstation Access Control

6.17.1 All workstations must use an access control system approved by Dr NDZ Municipality. In most cases this will involve password-enabled screen-savers with a time-out/after no-activity feature and a logon password to access the computer.

6.17.2 When a user leaves a workstation, the user is expected to properly log out of all applications and networks. This minimizes the opportunity for unauthorized users to assume the privileges of the intended user during the authorized user's absence.

6.17.3 Users will be held responsible for all actions taken under their sign-on.

Annexure A

ICT User Access Form



A Better Place for All

Enquiries

Tel: (039)833 1038 ext. 158

Email: spenganem@ndz.gov.za
: nxelem@ndz.gov.za

USER REGISTRATION FORM

Date: _____

Applicant's Full Name: _____

Employee Number: _____

Department: _____

Job Title: _____

PART A Please tick the box for the equipment required

New User	☐	Existing User	☐	Re-Instate User	☐	Delete User	☐	Disable User	☐	Enable User	☐
----------	--------------------------	---------------	--------------------------	-----------------	--------------------------	-------------	--------------------------	--------------	--------------------------	-------------	--------------------------

ICT Equipment:		Application Systems:	
Desktop	: ☐	SAMRAS SYSTEM	: ☐
Laptop	: ☐	Internet	: ☐
Printer	: ☐	Email	: ☐
3G Modem	: ☐		
Telephone Device	: ☐		
Cellphone	: ☐		
Storage Device	: ☐		
Other (Please specify)	: ☐		

I, _____, agree to, within three working days of my first access to the NDZLM network, read and abide by the ICT Usage Policy and to immediately seek clarity if there is any aspect I do not understand.

If I wish to move offices, I will ask the ICT to disconnect my computer.

I acknowledge and accept that all data, whether personal or corporate, I store on Municipality computers is the property of the Council. As such, I agree that the Municipality may view and manipulate this data.

When I leave the Department, I will return all software, supplies and equipment issued to me.

User Signature: _____ Date _____

Recommended by: _____ Signature: _____ Date _____

Approved by: _____ Signature _____

OFFICE USE

CREATED BY:	
USER NAME	
COMPUTER NAME	
MEMBER OF DOMAIN	
TELEPHONE PIN ISSUED	
TELEPHONE DEVICE ISSUED	
FAX TO EMAIL NUMBER	
EMAIL ADDRESS	
ASSET REGISTER SIGNED	
DATE REGISTERED	
VERIFIED BY and SIGN	

7. Policy Violations

7.1. Violations of this policy may result in disciplinary action, up to and including dismissal for employees, a termination of employment relations in the case of contractors or consultants, dismissal for interns, or suspension.

7.2. In the event of Dr NDZ Municipality incurring financial loss as a result of non-compliance, violation and / or disregard of this policy, Dr NDZ Municipality shall be entitled to institute legal proceedings to recoup the loss it has incurred from the employee / user and this shall be in addition to the disciplinary action that Dr NDZ Municipality would have taken against the employee.

8. Policy Review

- 8.1 This policy is subject to annual review or whenever it is deemed necessary by the Municipality, to ensure that it is aligned to prevailing resolutions, regulations and market conditions.

9. Publishing the policy

- 9.1 The policy shall be made available and accessible to all employees through manuals/hard copies.

10. Doctor Nkosazana Dlamini-Zuma Municipality Approval and Sign-Off

RECOMMENDATION

That the report be noted,
That the IT User Access Management Policy as part of the ICT Corporate Governance Framework be approved by Council.

Signature	Approved by	Date
		28 May 2026