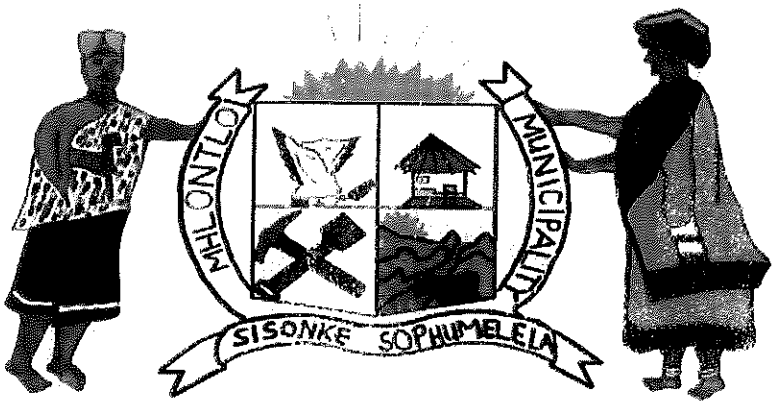


MHLONTLO LOCAL MUNICIPALITY ICT USER ACCESS MANAGEMENT POLICY

Financial Year: 2019 – 2020

TABLE OF CONTENTS PAGE

1. INTRODUCTION

The purpose of this policy is to prevent unauthorised access to the municipality's information systems. The Information and Communications Technology Security is becoming increasingly important to the Municipality, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

2. OBJECTIVE OF THE POLICY

The main objective of this policy is to provide the Municipality with best practice User Access Management controls and procedures to assist the Municipality in securing their user access and ensure the Institution has adequate controls to restrict access to systems and data, where it would apply to all Municipal users. This policy seeks to further ensure that it protects the privacy, security and confidentiality of the Municipality's information.
Formal procedures must control how access to information granted and how such access is changed. This policy also mandates a standard for the creation of unique ID and strong passwords.

3. AIM OF THE POLICY

The aim of this policy is to ensure that the Municipality conforms to standard user access management controls in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that risks associated to the management of user access are mitigated. This policy supports the Municipality's Corporate Governance of ICT Policy.

4. SCOPE

This policy is applicable to those who responsible for the management of user accounts or access to shared information or network devices. Such information can be held within a database, application or shared file space. This policy covers Municipal accounts as well as those managed by third party Service Providers and transversal systems.

The policy covers the following elements of user access management:

4.1 New user registration;
4.2 Terminated user removal;
4.3 User permission/role change request;
4.4 User access rights assignment for networks, operating systems, databases and applications;
4.5 Reviewing user access permissions; and
4.6 User and administrator activity monitoring.

5. POLICY APPROVAL AND AMENDMENT

The ICT Manager or delegated authority within the municipality is responsible for maintaining this policy. The policy must be reviewed on an annual basis and recommended changes must be approved by Council

6. DELEGATION OF RESPONSIBILITY

In accordance with the ICT Governance Policy, it is the responsibility of the Municipal Manager to determine the delegation of authority, personnel responsibilities and accountability to Management with regards to the Corporate Governance of ICT.

7. NEW USER REGISTRATION

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

7.2 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 this policy in Annexure B.

7.3 User access requests must be obtained from HR on registration of a new employee. The form must be sent to the middle 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. The form must then be sent back to HR for record keeping purposes.

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

7.5 All users must be assigned unique user IDs in order to ensure accountability for actions performed. Should shared accounts be required to fulfil a business function, this account must be approved and documented by the ISO.

7.6 The diagram below depicts the formal new user registration process to be followed.

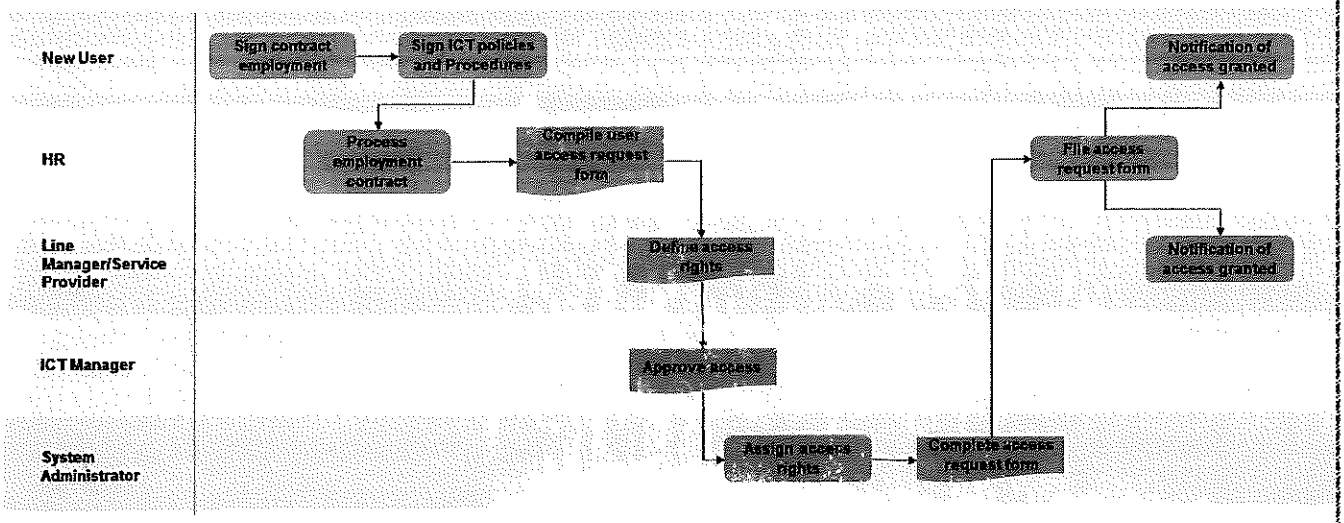


Figure 1: New user registration process

8. TERMINATED USER REMOVAL

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

8.2 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 authorization has been obtained by line manager.

8.3 Terminated user requests must be obtained from HR on the termination of an employee. 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 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. The form must then be sent back to HR for record keeping purposes.

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

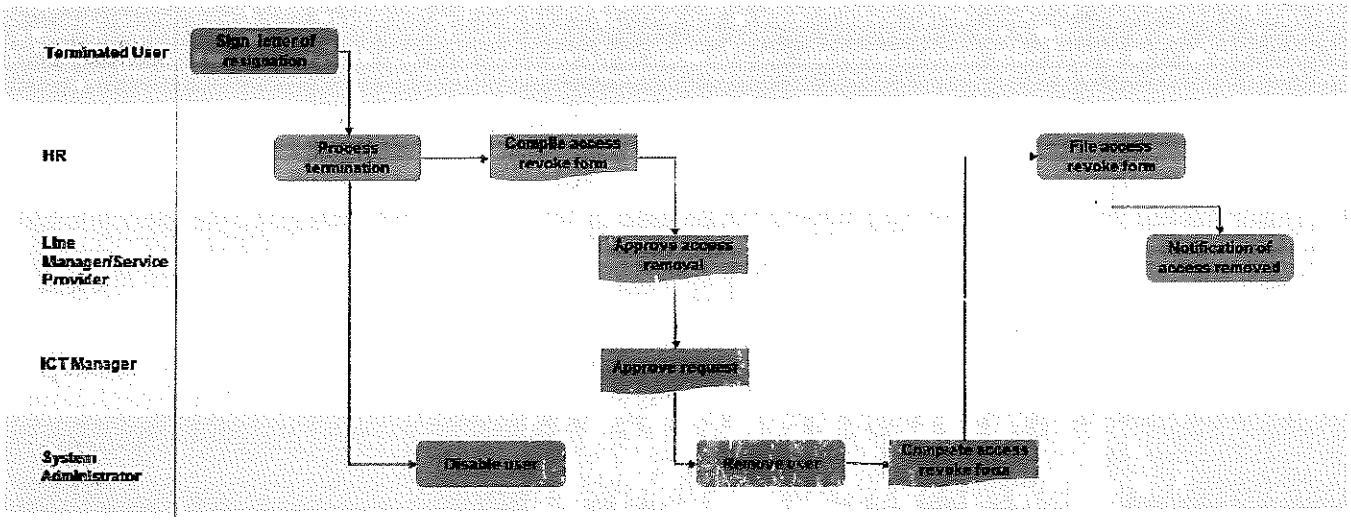


Figure 2: User termination process

9. USER PERMISSION/ROLE CHANGE REQUEST

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

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

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

9.4 User access change requests must be obtained from HR 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. The form must then be sent back to HR for record keeping purposes.

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

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

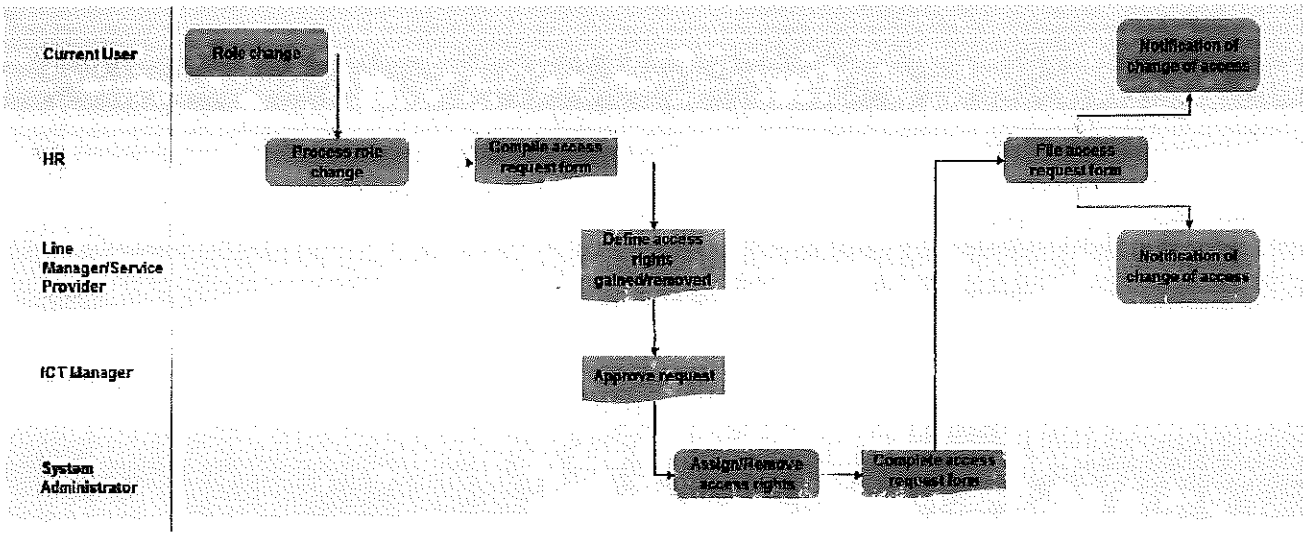


Figure 3: User permission/role change request process

10. GENERAL USER ACCESS RIGHTS ASSIGNMENT

10.1 Access rights include, but are not limited to:

(a) General office applications (E-mail, Microsoft Office, SharePoint, etc.);
(b) Department specific applications and/or databases;
(c) Network Shares;
(d) Administrative tasks;
(e) RAS/VPN Access;
(f) Wi-Fi;

10.2 Access must follow a "principle of least-privilege" approach, whereby all access is revoked by default and users are only allowed access based on their specific requirements.

10.3 The levels or degrees of access control to classified information must be restricted in terms of legislative prescripts.

10.4 Access rights must be assigned to a group/role. A user must then be assigned to that group. Access rights must not be assigned to individual users.

11. NETWORK USER ACCESS RIGHTS ASSIGNMENT

11.1 Access to the Municipality's network must only be allowed once a formal user registration process has been followed.

11.2 Access to Wi-Fi must only be provided to users who require access to the network throughout the Municipality, to fulfil their business function.

11.3 VPN access must only be granted to users who require the service to fulfil their business function.

11.4 Best practice states that VPN access must only be granted to employees who require remote access to a system in order to administer the environment.

11.5 Best practice states that VPN access must only be granted to employees who:

(a) Work remotely (Not at the office);

(b) Work overtime, or not within regular office hours.

11.6 It is the responsibility of the ICT Steering Committee to ensure all users must be made aware of the security risks and obligations associated with VPN access.

11.7 The ICT Manager must approve all hardware and software, owned by Municipal employees and service providers/vendors, if it is to be used for official purposes.

11.8 The ICT team must ensure that all mobile devices must be protected with a PIN.

12. OPERATING SYSTEM ACCESS RIGHTS ASSIGNMENT

12.1 Each system administrator must be given their own accounts within the administrator group. Should shared accounts be required to fulfil a business function, then this account must be approved and documented by the ISO.

12.2 The default guest account must be removed or renamed and disabled.

13. APPLICATION USER ACCESS RIGHTS ASSIGNMENT

13.1 Segregation of duties must be practiced, in such a way that application administrators cannot perform general user tasks on an application. This is to prevent any fraudulent activity from taking place.

13.2 Applications administrators must remain independent of the department utilising the application, with the exception of the ICT department.

14. DATABASE USER ACCESS RIGHTS ASSIGNMENT

14.1 The ICT Manager must limit full access to databases (e.g. system admin server role, db owner database role etc.) to ICT staff who need this access. Municipal employees who use applications may not have these rights to the application's databases.

14.2 The ICT Manager must ensure that Municipal employees who access databases directly (e.g. through ODBC) only have read access.

14.3 The ICT Steering Committee must approve all instances where Municipal employees have edit or execute access to databases.

14.4 The ICT Manager must review database rights and permissions on a quarterly basis (every 3 months). Excessive rights and permissions must be removed.

15. REVIEWING USER ACCESS AND PERMISSIONS

15.1 User access and user permissions must be reviewed every month by system administrators.

15.2 On a monthly basis, HR must send a list of all terminated employees for that month to the ICT department. This list must be used to ensure that all terminated users have had their access revoked. Should one or more terminated users still have access to the environment, an investigation into the finding must be conducted.

15.3 On a monthly basis, the ISO must review all users with administrative access to the environment and assess their rights for appropriateness. Should a user be found with excessive rights, a user access change request must be performed.

15.4 All reviews must be formally documented and signed off by the ISO. Documentation must be kept for record keeping purposes.

16. USER AND ADMINISTRATOR ACTIVITY MONITORING

16.1 User and administrator activity must be monitored through audit and event logging.

16.2 Every quarter (three months), system administrators and application owners must review audit and event logs for suspicious and malicious activities. A template for the reviewing of audit logs can be found in Appendix C of this Policy.

16.3 Dormant accounts should be disabled and a request to remove the access should be performed in line with section 11. User Permission/Role Change Request.

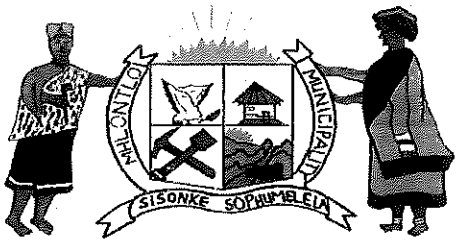
16.4 All reviews must be formally documented and signed off by the ISO. Documentation must be kept for record keeping purposes.

17. Policy Approval

This Policy was approved at a full Council Meeting held on 31 day of MAY (Month) 2019 (Year) at MHLONTLO Municipality.

Nonkunzelo Dyodi	Mayor	
Name and Surname	Designation	Signature
SOLOMON GATE JR	MM	
Name and Surname	Designation	Signature

18. ANNEXURE A: USER ACCESS MANAGEMENT FORM EXAMPLE



APPLICATION FOR ACCESS TO ICT EQUIPMENT

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:		**PROMUN:**	
LAPTOP:		**E-MAIL:**	
ACCESS TO PRINTER:		**GIS SYSTEMS :**	
3G MODEM:		**CELLPHONE:**	
VPN:		**TELEPHONE DEVICE AND/OR PIN CODE:**	
INTERNET:		**CELLPHONE:**	
OTHER:			

8

PART B: ACCEPT CONDITIONS OF USE OF COMPUTER SYSTEMS

The Mhlontlo Local Municipality strictly applies its ICT Usage Policy. You will not be allowed access to the network unless you sign the following undertaking.

I, _____, **agree to, within three working days of my first access to the MLM 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 Municipal Council. As such, I agree that the Municipality may view and manipulate this data.

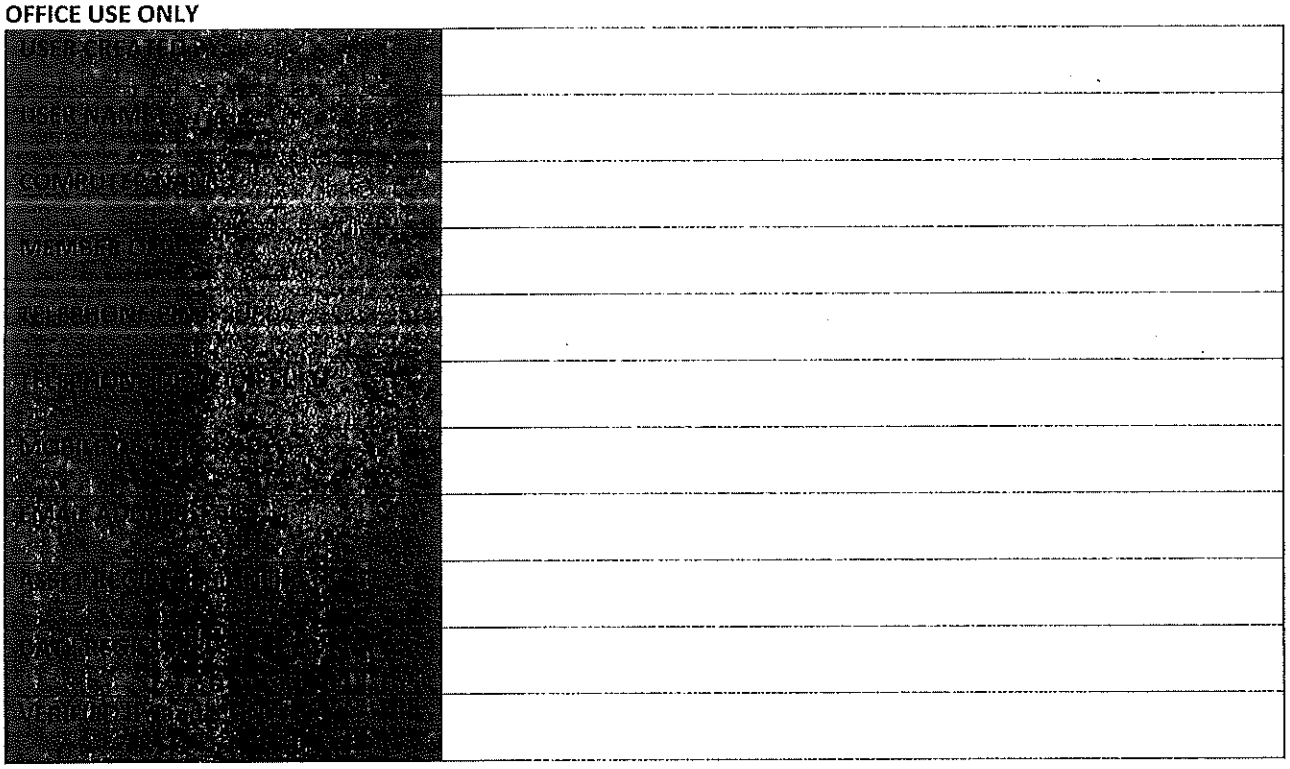
When I leave the Municipality I will return all software, supplies and equipment issued to me by the Municipality.

User Signature: _____ **Date:** _____

Recommended by: _____ **Signature:** _____ **Date** _____

Approved by: _____ **Signature:** _____ **Date:** _____

OFFICE USE ONLY



19. ANNEXURE B: OPERATING SYSTEM SECURITY SETTINGS

Security Configuration	Setting
Password Policy - General User Accounts	
Minimum password length	8 characters
Maximum password age	30 days
Password history	6 passwords remembered
Password complexity	Enabled
Account Lockout Policy - General User Accounts	
Account lockout duration	15 minutes
Account lockout threshold	3 attempts
Account lockout counter threshold	
	15 minutes
Audit Policy	
Account logon events	Failure
Account management	Success, Failure
Logon events	Failure
Policy change	Success, Failure
Privilege use	Success, Failure
System events	Failure
EVENT LOGS	

Application Log: Maximum log size (KB)	32 768
Application Log: When maximum event log is reached	Overwrite events as needed
Security Log: Maximum log size (KB)	81 920
Security Log: When maximum event log is reached	Overwrite events as needed
System Log: Maximum log size (KB)	32 768
System Log: When maximum event log is reached	Overwrite events as needed
Additional Settings	
Screen saver	Enable
Screen saver: Wait	10 minutes
On resume, display logon screen	Enabled
Accounts: Rename administrator account	Not Administrator or admin
Accounts: Rename guest account	Not Guest
Accounts: Guest account status	Disabled
Windows Firewall: Firewall state (Domain)	Enabled (1)
Windows Firewall: Firewall state (Private)	Enabled (1)
Windows Firewall: Firewall state (Public)	Enabled (1)

APPLICATION USER ACCESS REVIEW FORM		
MONTH OF REVIEW:		
EMPLOYEE NAME		
EMPLOYEE USERNAME		
JOB TITLE		
DEPARTMENT		
UNIT		
SYSTEM		
TYPE OF ACCESS		
DURATION		
	Start time: (if Applicable)	End Time:
USER DEPARTMENT/UNIT		
NAME		
COMMENTS		
SIGNATURE		
DATE		
ICT MANAGER		
NAME		
APPROVAL	YES ☐ NO ☐	
COMMENTS		
SIGNATURE		
DATE		
FOR ICT SERVICES UNIT ONLY		
EMPLOYEE USERNAME		
STATUS	**ACTIVE** ☐ **SUSPENDED** ☐ **DISABLED** ☐	
CREATION DATE		
CREATED BY		
ACCESS DETAILS		
SIGNATURE		

ANNEXURE C: AUDIT/EVENT LOG REVIEW TEMPLATE

ANNEXURE D: PROMUN RIGHTS REQUEST LETTER

POSTAL ADDRESS
P.O. Box 31
Qumbu
5180

PHYSICAL ADDRESS
96 Church Street
Qumbu
5180

Ifoni/Tel: 047-5537050
E-mail: pmalindi@mhlontlolml.gov.za
Imibuzo/Enquiries: P Malindi

Ifax/Fax: 047-5530189

BUDGET & TREASURY OFFICE

TO : CORPORATE SERVICES

CC : CHIEF ACCOUNTANT
: CHIEF FINANCE OFFICER

FROM : BUDGET REPORTING OFFICE

DATE : 22 JANUARY 2019

RE : **REQUEST FOR PROMUN RIGHTS**

This serves to request your good office to provide the B T O with the Promun rights Crd vat 201.p- Vat Extract New for MR K K Nolusu, Mr Q Gcelu and Mr M Ngedle.

Hope you will find the above in order.

Regards,

P. Malindi

Miss P Malindi
(Budget and Reporting Accountant)

Recommended,

Mr A. Ewana
(Chief Accountant)

Glossary of Abbreviations

Abbreviation	Definition
BYOD	Bring Your Own Device
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
VPN	Virtual Private Network
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.
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 Management Governance.
Dormant account	A user account that has not been accessed or used for 60 days or more
Middle 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.
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.