



THULAMELA MUNICIPALITY

USER ACCOUNT MANAGEMENT POLICY

DATE	1 July 2022
REVISION	0.6
Document ID	ICT-007-7718

Contents

Details	Pages
I) PREAMBLE	1
II) PURPOSE	1
III) SCOPE	1
1) User Account Management Procedures	2
2) Account Provisioning and De-Provisioning	3
3) Access Review Process	4
4) User Access Management Standards	4
5) Account Passwords Standard	4
6) Privileged Accounts	5
7) Account Passwords Guidelines	5
8) Responsible Use Standards	6
9) Violations	6
10) Access Control Business Requirements	7
11) System and Application Access Control Standard	7
12) User Registration	8
13) Monitoring User Access	8
14) Password Changes Administration	9
15) User Access Rights Review	9
16) User Password Management	9
17) Shared Accounts	10
18) Unattended User Equipment	10
19) Exceptions for Non-Compliant Systems and/or Users	10
20) Consequences of Non-Compliance	11
21) Policy Review	11
22) Effective Date	11
23) Signatures	11
Annexture (Systems Application Forms and Systems Matrix)	12

TAW MT

USER ACCOUNT MANAGEMENT

I) PREAMBLE

The Municipality should protect information assets from the risks created by both intentional and unintentional misuse of resources. The implementations of technology are diverse and complex (e.g. platforms, applications, operating systems, databases, email, etc.) and all of them have to be protected from unauthorised use or abuse.

The risks can, however, be minimized by following the good user account management practices prescribed by the International Organisation for Standardisation, the International Electro technical Commission on Information Technology – security techniques – Code of Practice for Information Security Management (ISO/IEC 27002:2005) and the Information Systems Audit and Control Association's guideline on access controls (G38). Criteria from these documents as outlined in this brochure could be of great value to the Municipality when performing self-assessments of access to their systems.

II) PURPOSE

The purpose of this document is to provide guidance in meeting the Municipality obligation to ensure that user access to systems and services is based upon authorization and that unauthorized access is prevented. This policy establishes standards for issuing accounts, creating password values, and managing accounts.

III) SCOPE

It is the responsibility of all system owners to determine appropriate controls, rules, access rights and restrictions for their information or information systems. They must assure that access is provided only to authorised users and that unauthorized access is prevented. Furthermore, it is important for all municipal staff, departments, internship, learnership, partners, contractors, service providers, volunteers or visitors using municipal facilities, services or IT systems to understand the need to ensure appropriate authorization to any system or service provided by the municipality.

1) User Account Management Procedures

These procedures should cover all stages in the life circle of user access, from the initial registration of new users to the final deregistration of users who no longer require access to information systems and services. All procedures should be documented and formally approved (signed and communicated). It should also be ensured that access control responsibilities, e.g. access request, access authorisation and access administration and monitoring, are segmented throughout the process.

2) Account Provisioning and De-Provisioning

A formal user access provisioning and de-provisioning process to assign or revoke access rights is available in the ICT Office and the following process is included:

Activity	Turnaround time (Max)
New User Application	Two working days (2)
Password Reset Request	Two Working hours (2)
User Modifications	Two Working hours (2)
User Access Revocation	Immediately after receipt

- The Password reset request activity may not be followed for Councilors and to all officials during pandemic periods, because of the realities of them not office based.
- All systems in the Municipality (e.g., Munsoft, Payday, TCS) shall be administered by a System Administrator except for National or Provincial System like eNaTIS.
- Level of access granted shall be verified and appropriate based on business purposes and other security controls;
- The allocation and use of privileged access rights shall be restricted and controlled;
- Unique user IDs shall be used in order to link actions to a specific individual;
- Shared user IDs shall only be permitted when critically necessary for business operations and the password shall be changed when a member of the group leaves;
- Unnecessary vendor-supplied default accounts shall be removed or disabled;
- For required vendor accounts, default passwords shall be changed following installation of systems or software;
- A central record of access rights granted shall be maintained;
- Access rights of all employees, internship, learnership and third party users shall be removed upon termination of employment, contract, or agreement.
- The Municipal line managers shall make decisions regarding access to their respective data (e.g., the CFO will determine who has access to revenue data, and what kind of access each user has). Account setup and modification shall require the signature of the requestor's supervisor and the CFO.
- The Municipality is responsible for resources and shall issue a unique account to each individual authorized to access that networked computing and information resource. It's also responsible for the prompt deactivation of accounts when necessary, i.e., accounts for terminated individuals shall be removed/disabled/revoked from any computing system at the end of the individual's employment or when continued access is no longer required; and the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location.
- The identity of users shall be authenticated before providing them with account and password details. If an automated process is used, then the account holder should be asked to provide several information items that in totality could only be known by the account holder. In addition, it is highly recommended that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access (e.g., user accounts used for email do not require an identity validation process as thorough as for those user accounts that can be used to modify department budgets).

TAN ME

- Passwords for new accounts shall NOT be emailed to remote users UNLESS the email is encrypted.
- The date when the account was issued shall be recorded in an audit log.
- All users with privileged access to all Municipal user accounts shall sign a Confidentiality Agreement that is kept in the file under the care of ICT.
- When establishing accounts, standard security principles of “least required access” to perform a function shall always apply, where administratively feasible, for example, a root or administrative privileged account must not be used when a non-privileged account will do.
- In case of Transversal or Financial Systems access, new users shall be registered by the System Controller upon completion of required documentation including the copy of identity document.

3) Access Review Process

A formal user access review process is stipulated as follows:

- Access rights shall be reviewed periodically;
- Documented audits of accounts with elevated privileges shall be conducted at least quarterly;
- Access rights of users who change roles or jobs within the organization shall be revised as appropriate;
- Accounts shall be removed or disabled in a timely manner for users who have left the organization;
- Privileged allocations will be checked to ensure unauthorized privileges have not been obtained;
- Specific procedures will be maintained to avoid unauthorized use of generic system administration user IDs.

4) User Access Management Standards

To assure only authorised access to their systems, owners should implement the following:

- A process for assigning, enabling, and revoking a user account
- A process for providing and revoking privileges associated with a user account
- A process for the controlled allocation and use of privileged access rights
- A process for managing the use of passwords, and, if implemented, managing encryption/cryptographic keys, and tokens
- A process for the review of user access rights at regular intervals
- A process for the removal and adjustment of access rights upon change of role, employment, contract, agreement or other status.

5) Account Passwords Standard

All Municipal-affiliated passwords should meet the requirements described below.

1. All passwords used must be strong and constructed using the following:

MT
TAN

- Minimum of eight (8) characters in length
 - Contains at least one character from each of the following four groups:
 - Lowercase letters
 - Uppercase letters
 - Numbers
 - Special character from this list !*+- / _#\$@%&\|?
2. Passwords must expire within an appropriate interval. Municipal defaults include:
- 30 days maximum per password
 - 1 day minimum per password
 - 24 enforcement to remember password history

3. Password System Requirements

- The system shall enforce the use of individual user IDs and passwords to maintain accountability.
- The system shall allow users to select and change their own passwords and include a confirmation procedure to allow for input errors.
- The system shall not display passwords on the screen when being entered.
- The system shall store and transmit passwords in a protected form.
- The system shall request a user's permission to store passwords.

6) Privileged Accounts

Accounts with elevated privileges should adhere to the standard password requirements and should be audited at least annually. NOTE: A privileged user account has powers within a system that are significantly greater than those assigned to the majority of users.

A formal authorisation process should be used to control the allocation of privileges in multi-user systems that require protection against unauthorised access. The following steps should be considered:

- The access privileges associated with each system product, e.g. operating system, database management system and each application, as well as the users to which they need to be allocated, should be identified.
- Privileges should be allocated to users on a need-to-use basis and on an event-by-event basis, i.e. the minimum required for their functional role and only when needed.
- An authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete.
- Privileges should be assigned to a different user ID than that used for normal business activities.
- Changes to privileged accounts should be logged for periodic review.

7) Account Passwords Guidelines

Consider these recommendations when selecting a password:

- Passwords should not contain your last name, first name, or email address.
- Avoid using dictionary words in passwords.

*MT
TAN*

- Consider using a “passphrase” that will be easy to remember and substitute some letters with numbers or symbols.

Follow these steps for keeping passwords secure:

- Treat passwords as confidential information and do not share them with others.
- Do not use passwords created to access Municipal systems for non- Municipal systems.
- Do not use the "Remember Password" feature in browsers and applications.
- Do not store passwords in a file unless the file is encrypted.
- If you know or suspect your account or password has been compromised, report the incident to ICT Office and change the password immediately.

General Password Usage:

- Keep password confidential.
- Avoid keeping a record of password, e.g. hard copy or electronic file.
- Change passwords whenever there is any indication of possible system or password compromise.
- Compose passwords that are:
 - easy to remember
 - of sufficient minimum length, e.g. six characters
 - not based on anything somebody else could easily guess or obtain using person-related information, e.g. names, telephone, dates of birth, etc.
 - not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries)
 - free of consecutive, identical, all-numerical, or all-alphabetical characters.
- Change passwords at regular intervals or based on the number of times access has been obtained. The passwords for privileged accounts should, however, be changed more frequently than normal passwords.
- Avoid the reuse or cycling of old passwords.
- Change temporary passwords at first logon.
- Never share individual user passwords among users.

8) Responsible Use Standards

Access to municipality information resources is a privilege granted to officials of the municipal community which carries with it the obligation to use these resources responsibly. General standards for responsible use of municipality information resources include respecting the privacy and rights of other users, sustaining the integrity of systems and related resources, and complying with all relevant policies, laws, regulations, and contractual obligations. Use of municipality information resources is conditioned upon adherence to the following principles of responsible use:

- Observe all government acts and laws, regulations, and policies of the municipality in the use of municipality information resources.
- Respect the privacy and personal rights of others.
- Respect and preserve the performance, integrity, and security of municipality information resources.
- Cooperate with the municipality to investigate potential unauthorized and/or illegal use of municipality information resources.

MT
TAN

- Protect the purpose of municipality information resources by ensuring that use does not result in improper commercial gain for the municipality, or personal commercial gain or private profit, except as allowed under the MFMA and corresponding policies and rules applicable to employees covered by the Public Service Act and related HR policies.
- Respect the intellectual property rights of others by ensuring that use of municipality information resources does not violate any copyright or trademark laws, municipality licensing agreements (including licensed software), or "Patent laws."

9) Violations

The following activities are specifically prohibited and considered violations of responsible use of municipality information resources:

- Use of another user's authentication credentials without his or her authorization;
- Accessing or transmitting information that belongs to another user or for which no authorization has been granted;
- An attempt to make unauthorized changes to information stored on a municipality information resource;
- Unauthorized copying of information stored on a municipality information resource;
- Tapping network or telephone lines in violation of any Government ACT or municipality policy;
- An action that jeopardizes the confidentiality, integrity or availability of a municipality computing, communication, or information resource;
- Use of municipality information resources that interferes with the work of other students, faculty, or staff or the normal operation of the municipality's computing systems;
- An attempt to bypass or aid others in bypassing the municipality's information technology security systems and mechanisms without the prior express permission of the owner of that system;
- Copying or distributing software licensed to the Municipality without authorization;
- Violation of federal, state or local laws, including copyright infringement;
- Use of municipality information resources for commercial purposes;
- Use of electronic mail messages or web pages that constitute invasion of privacy, harassment, defamation, threats, intimidation, or discrimination on a basis prohibited by federal or state law or municipality policies "Non-discrimination and Procedures for Addressing Reports of Discrimination."

10) Access Control Business Requirements

To assure only authorized access to information or information systems, the following principles should be considered:

- **Need-to-Know:** Only grant access to information needed to perform a task. Different tasks or roles may require different access profiles.
- **Need-to-Use:** Only grant access to IT equipment, applications, rooms, or procedures needed to perform a task, job, or role.

Access to networks and network services should be provided only to those authorized according to business need. Additional measures should be taken to limit access to network connections to sensitive or critical business applications from public or other off-site locations.

11) System and Application Access Control Standard

To provide adequate protection to their systems or applications, owners should implement the following:

- Access restrictions
- Secure logon procedures
- Password management protocols consistent with the Standard for Account Passwords
- Restrictions on any utility program that might be capable of overriding system and application controls
- Restrictions to access of program source code

12) User Registration

A formal user registration procedure / form for granting unique user account access to information systems and services is in place. Users will register as follows:

- For Email, Internet and Other Systems use *ICT Application Form*
- For Financial System use *Munsoft Application Form*
- For Personnel System use *Payday Application Form*

13) Monitoring User Access

- All accounts shall be reviewed at least quarterly by the IT Manager and bi-annually by the CFO to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status. The Information Security Officer may also conduct periodic reviews for any system connected to the Municipal network.
- All guest accounts with access to Municipality's computing resources shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

Monitoring of Access User Activities

- Those responsible for access to systems/applications/servers, etc protected by high-level super-passwords (or the equivalent) shall have proper auditable procedures in place to maintain custody of those "shared secrets" in the event of an emergency and/or should the super-password holder becomes unavailable.
- These documented procedures, which shall be appropriately secured, should delineate how these passwords are logically or physically accessed as well as who in the "chain of command" becomes responsible for access to and/or reset of the password.
- Activities done by the default account user (i.e. Guest, administrator, owner, root and system controller) should be monitored on a daily basis.
- All account logs shall be monitored weekly and administrator must sign log reports.

TAN MT

- After three failed attempts of login a user account will be disabled and the user has to follow the process of password reset. Failed attempts shall be logged unless the log information includes password information.
- All inactive accounts for 3 months shall be disabled and it will be activated after a user follows the user account modification/changes.
- All accounts that are inactive for 6 months shall be deleted from the systems.
- Accounts shall be monitored and reviewed.
- Password change events shall be recorded in an audit log and signed off by the ICT Security Officer.
- Controllers are accountable for instating, maintaining and communicating procedure to ensure the continuous control over access security in the department
- Such procedure should be specific in making sure that the users are responsible for their id's

14) Password Changes Administration

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 and should include, inter alia, the following:

- Changes should be communicated to information owners, users, super users, supervisors or system Controllers responsible for defining, granting, changing or revoking access privileges.
- The access rights of users who have changed job function, roles, responsibilities, etc. should immediately be removed or blocked.
- Procedures as for the registration of users should be followed when the status of a user changes.
- The Identity of users must be authenticated before providing them with password details. In addition, it is required that stricter levels of authentication (such as face-to-face) be used for those account with privileged access
- Whenever possible, passkeys should be used to authenticate a user when resetting a password or activating a guest account, and should comply with the above standards. Passkeys provide one-time access to a system or application and require the user to change to a password of their choice upon initial login.
- Where passkeys are not feasible, pre-expired passwords should be used
- Automated passwords resets are available and may be utilized, provided that a recognized and approved method is used, such as multiple, random challenge and response questions
- Passwords change events should be recorded in an audit log.

15) User Access Rights Review

The review of user's access rights is necessary to maintain effective control over access to data and information services. User's access rights should therefore be reviewed as follows:

- At regular intervals, e.g. every six months
- After any changes such as:
 - promotion
 - demotion
 - Transfer

M T
TAN

- termination of employment
- When moving from one section to another within the same Municipality.
- Authorisations for special privileged access rights should be reviewed at more frequent intervals, e.g. every three months.
- Privilege allocations should also be reviewed at more frequent intervals to ensure that no unauthorised privileges have been obtained.
- All changes to privileged accounts should be logged for periodic review.
- In every move that affect system use, ICT should be informed prior the move.

16) User Password Management

The allocation of passwords should be controlled through a formal management process and this process should include the following requirements as a minimum:

- Users should be required to sign an undertaking to keep personal passwords confidential. This signed statement could also be included in the terms and conditions of employment. (See the attached user access application form).
- If users are required to maintain their own passwords, they should be provided with a secure initial password, which they should be required to change immediately at first login.
- Procedures should be established to verify the identity of a user prior to providing the user with a new, replacement or temporary password.
- A secure procedure should be followed when granting users temporary passwords and the use of unprotected (clear text) electronic mail messages should be avoided.
- Temporary passwords should be unique and should conform to password standards.
- Users should acknowledge receipt of passwords.
- Passwords should never be stored on computer systems in an unprotected form.
- Default vendor passwords should be replaced as soon as the installation of systems or software has been completed.

17) Shared Accounts

Use of shared accounts is not allowed. However, in some situations, a provision to support the functionality of a process, system, device (such as servers, switchers or routers) or application may be made (e.g., management of file shares). Such exceptions will require documentation which justifies the need for a shared account; a copy of the documentation will be shared with Information Security Officer (ISO).

Each shared account must have a designated owner who is responsible for the management of access to that account. The owner is also responsible for the above mentioned documentation, which should include a list of individuals who have access to the shared account. The documentation must be available upon request for an audit or a security assessment.

18) Unattended User Equipment

All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well their responsibilities in regard to the implementation of such protection. Users should be advised to, inter alia:

MT
TAN

- terminate active sessions when finished, unless such sessions can be secured by an appropriate locking mechanism, e.g. a password-protected screen saver
- log computers off at the end of a session (i.e. it is not sufficient to merely switch off the PC screen or terminal)
- secure computers from unauthorised use by means of a key lock or an equivalent control, e.g. password access, when not in use.

19) Exceptions for Non-Compliant Systems and/or Users

Individuals that are unable to comply with the municipal ICT Account Management Policy must request an exemption from the Chairperson of the ICT Steering Committee. The Chairperson will process the request for final approval via the policy exceptions review. If after review, there is still disagreement over a decision, it may be appealed to the Municipal Manager. The decision of the MM will be final.

20) Consequences of Non-Compliance



Non-compliance of this policy may lead to disciplinary actions, legal liability as well as dismissal.

21) Policy Review

This policy shall be reviewed on 30 June 2025.

22) Effective Date

This policy comes into effect from the date of approval.

User Account Management Policy	
<input type="checkbox"/> Recommended by  Senior Manager: Corporate Services: Todani N.A	30, 06 /2022 Date
<input type="checkbox"/> Approved by  Acting Municipal Manager: Makumule MT	30, 06 /2022 Date



User Access Application Form

Surname										Full Names									
Preferred Name					Title					Initials					Personnel Number				
ID Number										Department									
Position/Designation										Unit									
Office Contact Number										Room Number									
+ 2 7 (0)										-									
Mobile Contact Number										Building Name									
+ 2 7 (0)										-									
Fax Number																			
+ 2 7 (0)										-									

Network Usage(✓ tick)

<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	eMail		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	MunSoft	
	Internet			Payday	
	Intranet only			Assetware	
	Trafman			Promise	
	Other			Venus	
	Other			TCS	

SUPERVISOR INFORMATION

Surname										Initial		Title		Position/Designation									
Mobile Number										+ 2 7 (0)				-									

Applicant Signature

Date of Application

IT Specialist (Office Use only)

	/ /20
Approved Username	Signature - IT Officials and Date

MT
TAN

ANNEXURE "A" USER DECLARATION

I (*print full name*) hereby declare that I have read and fully understand the User Account Management Policy of the Municipality of Thulamela, and that I undertake to adhere strictly to the said Policy.

I acknowledge that the details pertaining to specific instances may not be contained in this document, but should I be in any doubt as to how I should act, I will consult the User Account Management Policy document, or contact the ICT Section at the contact address or telephone number provided in the policy for advice.

I further acknowledge that my network access may at any time be revoked, or in the event that I abuse any facility available on the network, or in the event that I should pose a security risk to, or cause a security breach in the network of the Municipality.

SIGNED AT **ON THE** **DAY OF** **20**.....

USER:..... **WITNESS:**.....
Signature Surname, Initials and signature

Current / Private Email Address:

Personnel / ID Number:

Network User Login Name Provided (IT Official):

ANNEXURE "B" DISCLAIMER

"This message contains information that is confidential, legally privileged, and protected by law, and only for the use of the intended recipient. Any interception of the message is illegal, and if you are not the intended recipient, you may not peruse, use, disseminate, distribute or copy this message or any file attached to this message. Should you have received this message in error, please notify us immediately by return e-mail, and remove and delete any copy of this message.

Whilst the Municipality of Thulamela makes reasonable efforts to ensure that its system has been scanned and is free from viruses, the Municipality does not warrant that this message or any attachment to it is free from viruses, and it is incumbent upon the recipient to scan this message and any attachment to ensure that it is free from the viruses.

Views and opinions expressed in this message are those of the sender unless clearly stated as being that of the Municipality of Thulamela and therefore the Municipality does not accept any responsibility what so ever in regard of any damage this email may cause. Thank you in anticipation."

Payday Application Form



THULAMELA MUNICIPALITY PAYDAY USER ACCESS REQUEST FORM

No additions are acceptable. A new form has to be completed when functions are change and an automatic revocation of the previous rights will be implemented immediately.

Request No. (Date)		New User: <input type="checkbox"/>	Existing User: <input type="checkbox"/>
User Information:			
Surname			
First Name(s)			
Employee No.	Department		
Tel. Ext.	Email Address		

Access/Rights on PayDay:(Please, mark with an X)

Employee Menu

New Employee	<input type="checkbox"/>	Change Employee	<input type="checkbox"/>	Terminate Employee	<input type="checkbox"/>
Delete Employee	<input type="checkbox"/>	Employee Code Change	<input type="checkbox"/>	Delete Employee	<input type="checkbox"/>
Employee Code Change	<input type="checkbox"/>	Salary Screen	<input type="checkbox"/>	Batch Input	<input type="checkbox"/>
Recalculate	<input type="checkbox"/>	Human Resources	<input type="checkbox"/>	Leave	<input type="checkbox"/>
Clock Interface	<input type="checkbox"/>	Equity Module	<input type="checkbox"/>	mSCOA Module	<input type="checkbox"/>
Formula Menu	<input type="checkbox"/>	Report Menu	<input type="checkbox"/>	Backup Menu	<input type="checkbox"/>
Month End Procedures	<input type="checkbox"/>	Special Functions	<input type="checkbox"/>	Administrator Menu	<input type="checkbox"/>

Authorisation Information:			
User's Details		Signature	
Supervisor		Signature	
Manager HR		Signature	
Systems Administrator		Signature	
Given Username/Login Details:			
Company Number/Name	User Number	Date Created	

SUPERVISOR: Surname & Initials

Boxes Ticked

SUPERVISOR: Signature

Date

Page 1 | 2



**THULAMELA MUNICIPALITY
PAYDAY USER ACCESS REQUEST FORM**

No additions are acceptable. A new form has to be completed when functions are changed and an automatic revocation of the previous rights will be implemented immediately.

USER DECLARATION FORM

I (print full name) hereby declare that I have read and fully understand and informed of the importance of secrecy, confidentiality, risks, honesty in using the PayDay System within the signed and stipulated jurisdiction, binding system rights and demarcated areas to at all times guard against abuse of the system, doing corrupt activities and compromising security in any form.

I acknowledge that the details pertaining to specific instances may not be contained in this document, but should I be in any doubt as to how I should act, I will consult the related approved Policy documents of the Municipality, or contact the Line Manager or Supervisor or ICT Section for advice.

I further acknowledge that my system rights may at any time be revoked, or in the event that I abuse any facility available on the system, or in the event that I should pose a security risk to, or cause a security breach in the PayDay system of the Municipality. I undertake to adhere strictly to all HR and related Policies and standard approved.

SIGNED AT..... ON THE..... DAY OF 20.....

USER:.....
Signature

WITNESS:.....
Surname, Initials and
signature

Munsoft Application Form



V 0.1

THULAMELA MUNICIPALITY MUNSOFT USER ACCESS REQUEST FORM

No additions are acceptable. A new form has to be completed when functions are change and an automatic revocation of the previous rights will be implemented immediately.

Request No. (Date)	New User: <input type="checkbox"/>		Existing User: <input type="checkbox"/>	
Surname	User Information:			
First Name(s)				
Employee No.				
Tel. Ext.	Department			
	Email Address			

Consumer Debtors ☐:

Access/Rights on Munsoft: (Please, mark with an X)

- | | | |
|--|--|---|
| <p>1. Master Files <input type="checkbox"/></p> <p>1.1 Account files <input type="checkbox"/></p> <p>1.2 Account Tariffs <input type="checkbox"/></p> <p>1.3 Agreements <input type="checkbox"/></p> <p>1.4 Banking Details <input type="checkbox"/></p> <p>1.5 Credit Control <input type="checkbox"/></p> <p>1.6 Erf Master <input type="checkbox"/></p> <p>1.7 Extensions <input type="checkbox"/></p> <p>1.8 Housing Master Files <input type="checkbox"/></p> <p>1.9 Indigent Support <input type="checkbox"/></p> <p>1.10 Meter Master <input type="checkbox"/></p> <p>1.11 Meter On Hold <input type="checkbox"/></p> <p>1.12 Notes Master <input type="checkbox"/></p> <p>1.13 Pensioner Agreement <input type="checkbox"/></p> <p>1.14 S/Dry Charges Tariffs <input type="checkbox"/></p> <p>1.15 Valuation Master Files <input type="checkbox"/></p> <p>1.16 Transfer Of ACC Tariffs <input type="checkbox"/></p> <p>1.17 Transfer Of Ownership <input type="checkbox"/></p> <p>1.18 Inactivate Account <input type="checkbox"/></p> <p>1.19 Change Erf Number <input type="checkbox"/></p> <p>1.20 Change Meter Number <input type="checkbox"/></p> | <p>1.21 View Accounts on Erf. <input type="checkbox"/></p> <p>1.22 Link Accounts <input type="checkbox"/></p> <p>1.23 Available Accounts NOS <input type="checkbox"/></p> <p>1.24 Quick Account Create <input type="checkbox"/></p> <p>2. Transactions <input type="checkbox"/></p> <p>2.1 ACC Consolidation <input type="checkbox"/></p> <p>2.2 ACC Cons (OCO/Own) <input type="checkbox"/></p> <p>2.3 ACC Master Changes <input type="checkbox"/></p> <p>2.4 Agreement <input type="checkbox"/></p> <p>2.5 Agreement Adjustment <input type="checkbox"/></p> <p>2.6 Agreement Reversal <input type="checkbox"/></p> <p>2.7 Deposit Inc/Reimb <input type="checkbox"/></p> <p>2.8 Debit Inc/Reimb <input type="checkbox"/></p> <p>2.9 Dr/Cr Note Amend <input type="checkbox"/></p> <p>2.10 Housing Adj <input type="checkbox"/></p> <p>2.11 Indigent Support <input type="checkbox"/></p> <p>2.12 Interim Transactions <input type="checkbox"/></p> <p>2.13 Meter Adjustment <input type="checkbox"/></p> <p>2.14 Meter Bulk Adj <input type="checkbox"/></p> <p>2.15 Meter Disconnection <input type="checkbox"/></p> <p>2.16 Meter Reconnection <input type="checkbox"/></p> <p>2.17 Payment Transfer/Rever <input type="checkbox"/></p> | <p>2.18 Prmnt Trnfer Split <input type="checkbox"/></p> <p>2.19 Pensioner Support <input type="checkbox"/></p> <p>2.20 Re-Imbursement <input type="checkbox"/></p> <p>2.21 Transfer <input type="checkbox"/></p> <p>2.22 Write Off <input type="checkbox"/></p> <p>2.23 Write Off Reversal <input type="checkbox"/></p> <p>2.24 Auth Transactions <input type="checkbox"/></p> <p>2.25 Auth Billing <input type="checkbox"/></p> <p>2.26 Bulk Trans Import <input type="checkbox"/></p> <p>3. Statement Menu <input type="checkbox"/></p> <p>3.1 Create Statement Batch <input type="checkbox"/></p> <p>3.2 MMS Statement Batch <input type="checkbox"/></p> <p>3.3 MMS Delivery Import <input type="checkbox"/></p> <p>3.4 Email Statement Batch <input type="checkbox"/></p> <p>3.5 Email Delivery Import <input type="checkbox"/></p> <p>3.6 Print Statement Batch <input type="checkbox"/></p> <p>3.7 File Transfer <input type="checkbox"/></p> <p>3.8 Statement Batch Report <input type="checkbox"/></p> <p>3.9 Statement Range Print <input type="checkbox"/></p> <p>3.10 Statement Reprint <input type="checkbox"/></p> <p>3.11 Group ACC Statements <input type="checkbox"/></p> <p>4. Consumer Enquiries <input type="checkbox"/></p> <p>5. Meter Enquiries <input type="checkbox"/></p> |
|--|--|---|

SUPERVISOR: Surname & Initials

Boxes Ticked

SUPERVISOR: Signature

Date

Page 1 | 8

MT

6. P/Order – Create ☐

7. P/Order – Close ☐

8. Goods - Returned ☐

9. Project - Invoice ☐

10. Procurement Enquiries ☐

11. Scan Source Documents ☐

12. Source Documents Indexing ☐

13. P/Order – Delete

14. Creditor – Invoice

15. VM outside Docs

User's Details		Authorisation Information:	
Section Manager		Signature	
Chief Financial Officer		Signature	
Systems Administrator		Signature	
		Signature	

Given Username/Login Details:		
Username (1 st screen)	Pseudo Password	Date Created

**THULAMELA MUNICIPALITY
MUNSOFT USER ACCESS REQUEST FORM**

No additions are acceptable. A new form has to be completed when functions are change and an automatic revocation of the previous rights will be implemented immediately.



USER DECLARATION FORM

I (print full name) hereby declare that I have read and fully understand and informed of the importance of secrecy, confidentiality, risks, honesty in using the Munsoft Financial System within the signed and stipulated jurisdiction, binding system rights and demarcated areas to at all times guard against abuse of the system, doing corrupt activities and compromising security in any form.

I acknowledge that the details pertaining to specific instances may not be contained in this document, but should I be in any doubt as to how I should act, I will consult the related approved Policy documents of the Municipality, or contact the Line Manager or Supervisor or ICT Section for advice.

I further acknowledge that my system rights may at any time be revoked, or in the event that I abuse any facility available on the system, or in the event that I should pose a security risk to, or cause a security breach in the Munsoft system of the Municipality. I undertake to adhere strictly to all Finance and related Policies and standard approved.

SIGNED AT..... ON THE..... DAY OF 20.....

USER:.....
Signature

WITNESS:.....
Surname, Initials and signature

SUPERVISOR: Surname & Initials

☐

Boxes Ticked

SUPERVISOR: Signature

Date

Page 8 | 8



THULAMELA LOCAL MUNICIPALITY

Password Reset Request form

User Details		Request Date: / /	
First Name(s)			
Surname			
Employee Number			
Department			
Section			
Office Tel			
System to Reset	Mobile Contact		
I hereby Request that my Password be reset for the following reason(s)			
Applicant Signature			

Supervisor's Details	
Surname & initials	
Office Telephone	Mobile Number

Supervisor's Signature

Date

ICT-14