**UMTSHEZI MUNICIPALITY**



**USER ACCOUNT MANAGEMENT PROCEDURES**

User Account Management Procedures

**Approval and Version Control**

|  |  |  |
| --- | --- | --- |
| **Approval Process:** | **Position or Meeting Number:** | **Date:** |
| Originator |  |  |
| Recommended by Director of Corporate Services |  |  |
| Recommended by EXCO |  |  |
| Approved by Council | Res 271.06.14 | 14 June 2014 |
| Effective |  |  |
| Review Frequency: Once a year (i.e. Annually) | Res 119.07.15 | 14 July 2015 |
| Version Number |  |  |

Table of Contents

[1. Purpose 4](#_Toc377646939)

[2. Scope 4](#_Toc377646940)

[3. User Access Procedures 5](#_Toc377646941)

[3.1. New Users or Change User Access 5](#_Toc377646942)

[3.2. Re-instate User Access 6](#_Toc377646943)

[3.3. Termination of User Access 7](#_Toc377646944)

[3.4. Password Resets 8](#_Toc377646945)

[4. Periodic Review of User Profiles and Access Rights 9](#_Toc377646946)

[5. Enforcement 9](#_Toc377646947)

[6. Appendices 9](#_Toc377646948)

[A. User Access Request Form 9](#_Toc377646949)

# Purpose

The purpose of the Umtshezi Municipality User Account Management Procedure is to maintain an adequate level of security to protect Umtshezi Municipality data and information systems from unauthorised access. This procedure defines the rules necessary to achieve this protection and to ensure a secure and reliable operation of Umtshezi Municipality information systems.

# Scope

This procedure document applies to all computer and communication systems owned or operated by Umtshezi Municipality and its subsidiaries. Similarly, these procedures apply to all platforms (operating systems) and all application systems.

# User Access Procedures

## New Users or Change User Access

* + 1. A user will request access or change of access either to the network or to an application from the IT Officer.
		2. The User Access Form (see Appendix A) will then be sent to the users’ manager or be provided directly to the user.
		3. The user must then complete the User Access Form, sign it and submit the form to his / her Manager for approval.
		4. The users’ Manager will review the access applied for by the user to determine if the access requested is in accordance with the system function required for the staff member to perform his/her duties.
		5. The Manager will then sign and date the form as acknowledgement of approval.
		6. If the user requires access or modification of his/her access to Venus, the user must select what type of access is required and submit the form to the CFO.
		7. The CFO must review the access permissions selected by the user and provide approval of said accesses before access to Venus can be granted/modified by the IT Officer.
		8. The completed and approved User Access Form must then be submitted to the IT Officer.
		9. The IT Officer will review the User Access Form to ensure that the information is complete and valid authorisation has been provided in accordance with the system security baseline for each application to ensure that the access requested does not provide excessive system access or conflicting roles.
		10. The IT Officer must also establish whether the employee is entitled to the access / requires modified access (i.e. relevant enquiries must be made through Human Resources to validate employment accordingly).
		11. The IT Officer must sign and date the form as acknowledgement of approval.
		12. The IT Officer will then grant access as per the User Access Form and will use the standard naming convention that is stipulated overleaf.
		13. The following user account naming conventions must be used to ensure user ID’s are unique to enable easy identification of users allocated access and also prevent the possibility of duplicate system account ID’s.

|  |  |  |
| --- | --- | --- |
| Ref No | Application | Naming Convention |
| 1 | All Systems | Full first name and surname initial – example joeb (Joe Blogg) |

* + 1. The IT Officer will then notify the user that access has been granted / modified via email or telephone.
		2. The User Access Form must be filed and retained for audit purposes.
		3. Where the system functionality allows it, the user must change their password at their first subsequent login.

 **Note: If an individual is acting in a position that requires elevated access then proof of said acting position is required.**

1.

## Re-instate User Access

* + 1. The re-instate user option will be used when a user is on leave for an extended period of time. The following are examples of when this procedure can be used but is not an not exhaustive list:
			1. Maternity leave;
			2. Sabbatical; and
			3. Suspension.
		2. The Human Resources (HR) department must inform the IT Officer when an employee will be taking extended leave.
		3. Upon notification from the HR department, the IT Officer will disable the employee’s user account on his/her last working day.
		4. When the user’s account needs to be re-instated, the user’s Line Manager must log a call with the IT Officer.
		5. The User Access Request Form (see Appendix A) will then be sent to the user’s Line Manager by the IT Officer.
		6. The user’s Line Manager will fill in the users’ details under ‘User information’ in the User Access Request Form and will tick the box ‘Re-Instate User’.
		7. The completed User Access Request Form must be returned to the IT Officer.
		8. Upon receiving the User Access Request Form, the IT Officer will review the User Access Request Form to ensure that the information is complete and valid authorisation has been provided.
		9. The IT Officer must also establish whether the employee is entitled to have his/her access re-instated (i.e. relevant enquiries must be made through Human Resources).
		10. The IT Officer must sign and date the form as acknowledgement of approval.
		11. The IT Officer will re-instate the employees’ access as per the User Access Request Form.
		12. The IT Officer will then notify the relevant Line Manager that the employees’ access has been re-instated.
		13. The User Access Request Form must be filed and retained for audit purposes.

## Termination of User Access

* + 1. The Human Resources (HR) department must send a monthly Terminations Listing Report to the IT Officer to identify employees whose access must be disabled at month end.
		2. Upon receiving the Termination Listing Report, the IT Officer must then disable all terminated employee’s access on the relevant systems immediately.
		3. The IT Officer will then notify the relevant Managers via email that the terminated employees have had their access disabled on the relevant system(s) accordingly.
		4. The disabled user accounts must be moved to the dormant group and deleted after 90 days have elapsed.

## Password Resets

* + 1. The password reset option will be used when a user has forgotten his/her password or if a user’s account has been locked due to multiple failed login attempts.
		2. When a user requires their password to be reset or account to be unlocked, the user will log a call with the IT Officer.
		3. The IT Officer must verify if the account was locked due to the user entering his/her password incorrectly on three (3) consecutive occasions or if there was an unauthorised attempt to gain access.
		4. If the IT Officer suspects that an IT security incident has occurred, he/she must invoke the Helpdesk and Incident Management Policy.
		5. The User Access Form (see Appendix A) will then be sent to the user by the IT Officer.
		6. The user must complete their details under ‘User information’ on the User Access Request Form and tick the ‘Password Reset’ box.
		7. The completed User Access Request Form must be returned to the IT Officer.
		8. Upon receiving the User Access Request Form, the IT Officer will review the User Access Request Form to ensure that the information is complete and valid authorisation has been provided.
		9. The IT Officer will reset the password or unlock the account upon verification of the user’s identity.
		10. The “change password at next logon” setting must be ticked and enforced by the IT Officer, so that the user will be forced to change their password when they next logon to the network.

# Periodic Review of User Profiles and Access Rights

* 1. A review of all user accounts must be performed on an annual basis by the organization.
	2. This is done by verifying if the user’s permissions and access rights are commensurate with their current role and responsibilities.
	3. The IT Officer will provide the access rights of staff to the Line Managers for review.
	4. The Line Managers must flag inappropriate access and sign-off the access lists. This must be retained by IT as evidence.
	5. Where inappropriate access is identified, the access should be removed or amended as appropriate by the IT Officer.
	6. The review must also ensure that user IDs are linked to specific individuals by specifying the name and surname of the user concerned against each user ID.
	7. The review must also include the identification of inactive/ dormant user accounts. An account is deemed ‘inactive’ where it has not been used within 90 days. Inactive accounts must be moved to the “Dormant” group and disabled. This would only apply for User Accounts and not System Accounts.
	8. Appropriate evidence of the review must be retained and filed.

#

# Enforcement

If any Umtshezi Municipality staff member is found to have breached this procedure document, they may be subject to disciplinary action, up to and including termination of employment. Any violation of this procedure document by a temporary worker, contractor or supplier may also result in the termination of their contract or assignment accordingly.

# Appendices

### User Access Request Form

|  |  |  |
| --- | --- | --- |
|  | **Umtshezi Municipality****User Access Request Form** |  |

**Appendix A: User Access Request Form**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| New User |  | Change User Access |  | Re-Instate User |  | Delete User |  | PasswordReset  |  |

|  |
| --- |
| **User Information:** |
| First Name |  | Last Name |  |
| Employee Code |  | Department |  |
| Job Tittle |  | Telephone Number |  |
| E-mail address |  | Line Manager |  |

|  |
| --- |
| **Application Access Requested:** |
|  Internet Mail Network Venus OtherIf other, specify \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

| **Access Required:** |
| --- |
| **Financial System Modules** | **Read Only** | **Read/Write** | **Add** | **Remove** | **Modify** |
| **My Desktop** |  |  |  |  |  |
| **Common** |  |  |  |  |  |
| **General Ledger** |  |  |  |  |  |
| **Accounts Receivable** |  |  |  |  |  |
| **Accounts Payable** |  |  |  |  |  |
| **Annuity Billing** |  |  |  |  |  |
| **Contract Management** |  |  |  |  |  |
| **Inventory** |  |  |  |  |  |
| **Order Entry** |  |  |  |  |  |
| **Procurement** |  |  |  |  |  |
| **Job Costing** |  |  |  |  |  |
| **Point of Sale** |  |  |  |  |  |
| **Fixed Assets** |  |  |  |  |  |
| **Alert Management** |  |  |  |  |  |
| **Inventory Issue** |  |  |  |  |  |
|  |  |  |  |  |  |
| **HR System Modules** | **Read Only** | **Read/Write** | **Add** | **Remove** | **Modify** |
| **Equity** |  |  |  |  |  |
| **Utilities** |  |  |  |  |  |
| **Reports** |  |  |  |  |  |
| **Company** |  |  |  |  |  |
| **Employees earnings and deductions** |  |  |  |  |  |
| **Payroll** |  |  |  |  |  |
| **Leave** |  |  |  |  |  |
| **Interfaces** |  |  |  |  |  |

|  |
| --- |
| **Authorisation Information:** |
| Authorised by Line Manager |  | Signature |  | Date |  |
| Authorised by CFO |  | Signature |  | Date |  |
| Authorised by IT Officer |  | Signature |  | Date |  |
| Access Granted by |  | Signature |  | Date |  |

|  |
| --- |
| **Additional Comments** |
|  |