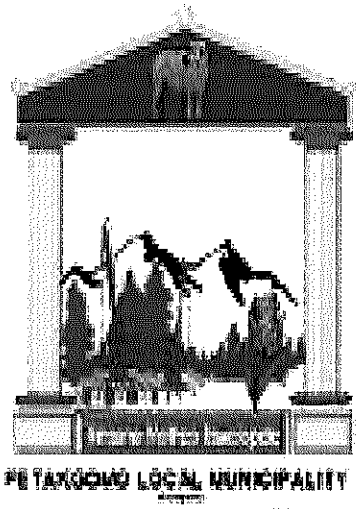
Fetakgomo Local Municipality



Council Resolution No. C76/2016

Draft of IT User Access Management Policy & Procedure

Fetakgomo Local Municipality

User Access Management Policy and Procedure

Table of Contents

Purpose:	This Policy and Procedure intends to protect the Confidentiality, Integrity, and Availability of Fetakgomo Local Municipality's Information and Information Systems by preventing unauthorised user(s) access to Fetakgomo local Municipality Information and Information Systems. This document establishes a procedure in accordance with the Access Control policy for the authorization, modification, review, and revocation of a user's access "Business Applications" Munsoft and VIP. It also describes requirements for training those involved in the access control process. This Policy should be read in conjunction with Security policy
Reference:	User Access Management Policy and Procedure

1 Scope:

This Policy applies –

(a) to each employee of Fetakgomo Local Municipality ; and

(b) where appropriate, to any other person provided access to Fetakgomo Local Municipality's computer resources for whatever reason, (together referred to as "users").

This Policy applies –

(a) to the use of any Fetakgomo Local Municipality's computer resource;

(b) to Internet access where access has been authorised in terms of Fetakgomo Local Municipality's Internet Access Policy;

(c) where appropriate, to any official work, whether undertaken from the offices of Fetakgomo Local Municipality or off-site; and

(d) any remote sites of access, if applicable.

2 Responsibility

2.1 the responsibility for the implementation and the effectiveness of this policy document is shall liaise with Information Technology Personnel

3 Additional Resources:

Other police that can be used in conjunction within this are:

- Integrated Development Plan
- Security policy and Procedure
- Supply chain Management
- Municipality Finance Management Act.
- User Registration form ITUFTM-REG-F2014

4 Definitions

Identification is the method used to distinguish one user from all others. Identification techniques provide a means of providing authorised entry to the Municipality's resources such as workstations, networks and applications. Identification is closely linked to authentication (see below).

The most commonly used form of "electronic" identification is a user ID. Common physical forms of identification include the ID Document or card, driver's license, passport and similar.

Password: A password is a unique alphanumeric string only known to the user. A password is traditionally associated with a user ID to identify and then authenticate a user.

Authentication is the act of verifying the identity of a user or process. It is the process of determining whether someone or something is, in fact, who or what it is declared to be. It answers the question: "Are you who you say you are?"

Authorisation answers the question: "Are you allowed to do what you are asking or trying to do?" Requirements for user and prohibitions against use, of resources vary widely throughout the Municipality. Some information may be accessible by all users, some may be accessible by several groups or

departments, and some may only be accessible by a few individuals. Authorisation addresses these requirements for varied access levels.

5 Policy Statement

5.1.1 User access management must be created to prevent unauthorised access to information systems.

Objective: *to control the allocation of access rights to information and information systems including granting and revoking of access to all information systems and services.*

5.1.2 All users accessing the Municipality information systems (Munsoft or VIP) must be registered with the IT unit and deregistered once their term of service is over.

5.1.3 Generic or group ID's shall not be permitted other than in exceptional circumstances.

5.1.4 The allocation of privilege rights (e.g. administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Manager. They shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.

5.1.5 All users of the municipality information systems must ensure that password are secured and reviewed on regular basis. The password must be greater than 8 characters and must contain capital letters, number and special character e.g. P@$$w8%d

5.1.6 A formal process shall be conducted at regular intervals by system owners in conjunction with the Information technology Manager to review users' access rights including the VPN access for Munsoft. The review shall be logged and the Information Technology Manager and System Owner shall sign off the review to give authority for users' continued access rights. Each department need to identify a System owner for their system e.g. Munsoft ad VIP system owners.

5.1.7 Access for remote users shall be subject to authorization by Information Technology Manager and no uncontrolled external access shall be permitted to any network device or networked system.

5.1.8 Connections to remote systems must be authenticated by Information Technology personnel to establish the identity and authenticity of remote systems.

5.1.9 Routing controls shall be implemented to ensure that computer connections and information flows do not breach the access control policy of the business applications.

6 User Account Management Procedure

6.1 Account Management

6.1.1 The Information Technology Manager and System Owners manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. They also review information system accounts at least monthly. All other accounts are disabled per the applicable Operating System hardening guide.

6.2 Account Creation/Modification

6.2.1 Upon receipt of a the user Registration form ITUFTM-REG-F2014 A User's Supervisor will determine whether a User needs access to a Business Application or when modification of a User's access to a Business Application is necessary.

6.2.2 In either case, the User's Supervisor will acknowledge appropriate access based on legitimate business need and will relay the request for access or modification of access to the System Owner.

6.2.3 The User's Supervisor is responsible for ensuring that the User will attend any training available for the Business Application(s) as related to the User's job function and the access level requested.

6.2.4 The System Owner will validate the request and submit it to the Information Technology Manager. The Information Technology Manager will verify the User's active status in the affected Application(s) and the authority of the System Owner (typically, by appropriateness of job title).

6.2.5 The Information Technology Manager or Information Technology Personnel will grant access, set up the accounts and notify the User, the User's Supervisor or the System Owner that access has been granted.

6.3 Review of Access

6.3.1 Access to Applications will be reviewed periodically in accordance with the following procedures:

6.3.2 **Deactivation of Inactive Account**

6.3.2.1 Every six months the Information Technology Manager will generate a report of all accounts that have had no activity for 180 consecutive days. The Information Technology Manager will distribute this report to the System Owner(s). The System Owner(s) will note on the report which accounts must be disabled or deleted, then will submit the report to the office of Information Technology Manager. The Information Technology Manager will disable or delete the account to prevent further activity. If access is disabled rather than deleted, the Information Technology will make an appropriate log entry to explain the reason.

6.3.3 **Continued Appropriateness of Access**

6.3.3.1 Annually, the Information Technology Manager will be responsible for extracting a sample of the active User base from each Business Application and surveying the Users' Supervisors or System Owners to determine whether access of each User in the sample remains appropriate for a legitimate business need. Based on the response to that survey, the Information Technology Manager may leave unchanged, modify or terminate a User's access. An appropriate log entry will be made to note the review of the account, including the date and the action taken. The Information Technology Manager will notify the System Owner of any access changes.

6.3.4 **Review of Access Roles When Modified**

6.3.4.1 Whenever an access role is modified to reflect a change in business

6.3.4.2 practice or system organization, the Information Technology Manager and possibly the System Owner for the applicable Business Application will review its scope of access and

Revocation of Access

6.3.5 When a User leaves a position for which s/he has been granted access to a Business Application, that access must be revoked as soon as practicable, as provided below.

6.3.6 Upon a change in position, whether for transfer, promotion, resignation, termination, or for any reason a User no longer requires access to a Business Application, that User, the User's Supervisor or other responsible person should notify the Information technology office in writing. The Information Technology office will revoke access and deactivate the account immediately upon notification. In the event of a change in position, the Information Technology Manager will modify or revoke and re-establish an account upon receiving appropriate authorization as described above under the heading "Account Creation/Modification." The Information Technology Manager will notify the User's Supervisor and System Owner after the User's account has been modified or removed.

6.3.7 Quarterly, the Information Technology Manager will request a report extracted from VIP indicating

6.3.8 Users who have changed positions within Fetakgomo Local Municipality. The Information Technology Manager is responsible for checking any reported User's current access level to determine if access is still valid. The Information Technology Manager is responsible for continued access notations, account modification and/or removal from the Business Application.

6.3.9 The Information Technology will retain report records of modified and deactivated accounts.

7 General

7.1 System security

Each user has a duty to safeguard the Municipality's computer resources and data. This means that, amongst other things, users must not –

(i) discloses or share their user identity or password with any other user or person;

(ii) log out of the network (you need not necessarily switch off your computer) when you are away from your desk for substantial periods of time or at the end of the working day; and

(iii) check any stiffy disks or CDs for viruses (users should contact the Information Technology Office to ensure that disks and CDs are checked for viruses).

(i) download, upload or install any software, whether licenced or unlicensed, games, public domain software, freeware, shareware or demonstration software, onto Fetakgomo Local Municipality computer systems without express prior authority;

(ii) download, distribute or store text, code, images or other material in contravention of copyright or any other intellectual property rights;

(iii) attempt to intercept data without authority;

(iv) attempt to access or view data or files of other users without authority;

(v) modify data or files of other users without authority;

(vi) attempt to access confidential data without authority;

(vii) damage or delete any data;

(viii) attempt to access restricted areas of the computer system without authority;

(ix) use the Municipality's computer resources to undertake any form of hacking (i.e. attempting to probe the security of or penetrate a remote site or computer without authority);

(x) intentionally introduce a virus, worm or other form of malicious attack;

(xi) intentionally impair the functioning of a computer system; and

(xii) store personal files on the Municipality's computer system.

7.2 Monitoring

7.2.1 Systems, Email, including personal emails, Internet access and the use of other computer resources may be monitored, intercepted and/or logged without notice. Users should, therefore, have no expectation of privacy in respect of any aspect of their use of the Municipality's computer resources, provided that use of the computer resources will not be monitored otherwise than in terms of this Policy.

Monitoring will take place for the following purposes:

(i) network security / maintenance;

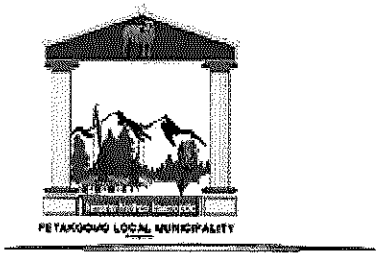
(ii) obtaining evidence of official communications;

(iii) ensuring adherence to procedures and standards;

(iv) accessing information during the user's absence; and

(v) detecting or preventing unauthorised or unlawful use of computer resources.

Appendix A



ITUFTM-REG-F2014

IT Access Request Form					
Section A : User and Departmental Information					
Last Name:		First Name:		Employee No.	
Initials :	Office Name/No:	Division Name:			
Department:		Supervisor			
Tel No:		Email:			
Section B : Access Required					
New User ☐	Delete User ☐	Update User's details ☐	Change User's Password ☐		
NETWORK ☐	MUNSOFT ☐	VIP ☐			
INTERNET ☐	E-MAIL ☐	GIS ☐	DOMAIN ☐	AUTO CAD ☐	PASTEL ☐
Application	Access Level	Training Required?	Training Complete?	Grant or Revoke	
Comments:					
Section C : Access Request Approval					
Completed by: User		Date:			

Authorized by: System Owner/ Supervisor		Date:	
Access Granted by: IT Personnel		Date:	

Practice Notes

1. Security Practice Notes

1.1 Practice Notes for Password use [Go back]

1.1.1 Users must be educated to follow good security practices in the selection and use of passwords.

1.1.2 Users must be advised to:

(a) keep passwords confidential;

(b) avoid keeping a paper record of passwords, unless this can be stored securely;

(c) change passwords whenever there is any indication of possible system or password compromise;

(d) select quality passwords with a minimum length of eight characters which are:

(i) easy to remember;

(ii) not based on anything somebody else could easily guess or obtain using person-related information, e.g. names, telephone numbers, birth dates, *etc.; and*

(iii) free of consecutive identical characters or all-numeric or all-alphabetical groups.

1.1.3 Where ever possible, password criteria should be enforced by program code.

1.1.4 change passwords at regular intervals or based on the number of accesses (passwords conferring higher privileges should be changed more frequently than normal passwords) and avoid re-using or cycling old passwords. Where possible, this should be enforced by program code;

1.1.5 change temporary passwords at the first log-on. This should also be enforced by program code;

1.1.6 not include passwords in any automated log-on process, e.g. stored in a macro or function key; and

1.1.7 never share passwords.

Appendix B

Index

Mamphekgo KK

Council Chairperson

22-03-2016

Date