IT User Access Management Policy

Date Approved	Version	Resolution Number
30 June 2016	1	10.3.2
28 July 2017	2	019/OCM/17

The Information Technology Manager

Senqu Local Municipality

19 Murray Street

Lady Grey

Telephone (051) 603 1300

Facsimile (051) 603 0445

Website: www.senqu.gov.za

IT User Access Management Policy

As a government institution, Senqu Municipality must implement an IT User Access Management Policy to maintain an adequate level of security to protect the Municipality's data and information systems from unauthorised access and to ensure a secure and reliable operation of the Municipality's information systems.

Full Title	**Senqu Municipality's IT User Access Management Policy**
Short Title	IT User Access Management Policy

Resolution: 019/OCM/17	**Approved 28 July 2017**

Table of Contents

Resolution: 019/OCM/17	Approved 28 July 2017

1. Version Control

Full Title	**Senqu Municipality IT User Access Management Policy**
Short Title	User Access Management Policy
Author(s)	Mr R Johl
Version	0.1

Authors	Mr R Johl (PWC) & Ms. Magdalena Oertel (Senqu)
Version	01
Authorised By	Council
Authorisation Date	30 June 2016
Effective Date	1 July 2016

Revised	Ms. Magdalena Oertel (Senqu Municipality)
Version	02
Authorised By	Council
Authorisation Date	28 July 2017
Effective Date	1 July 2017

Resolution: 019/OCM/17	**Approved 28 July 2017**

2. Definitions

Term	Meaning
IT	Information Technology
ICT	Information and Communication Technology
Municipality, the	Senqu Municipality
CFO	Chief Finance Officer
LAN	Local Area Network
VPN	Virtual Private Network
SSH	Secure Shell
FTP	File Transfer Protocol

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 unauthorised 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 authorisation 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 authorised 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 Senqu Municipality and all contractors, consultants, temporary employees and business partners.

6. Policy

6.1 Authorised Users

6.1.1 Only authorised 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 Senqu Municipality's 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 authorised individuals should access the system.

6.3.2 The warning message must clarify that the system is a private network or application and unauthorised 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.

Resolution: 019/OCM/17	Approved 28 July 2017

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 Senqu Municipality's information systems must sign a compliance statement prior to issuance of a user ID. Refer to the Senqu Municipality's IT Security Policy for further details.

6.7.2 A signature on this compliance statement indicates the user understands and agrees to abide by Senqu 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 IT 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 IT 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 Senqu 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 IT 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 Senqu 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 IT 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 Senqu 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 IT Manager, these updates may be required to run more frequently due to business requirements.

6.13.3 Any authorised user using a remote computing device outside the firewall must use the VPN to send and receive Senqu Municipality's email or to access the Internet and Intranet accordingly. No Senqu Municipal email may be sent using third-party email services (including, but not limited to, Gmail, Hotmail, Webmail, etc.).

6.13.4 Any authorised 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 Senqu Municipality's LAN shall not do so while still connected to any other network.

6.13.6 All employees requiring remote access to Senqu Municipality's LAN must obtain approval from the IT Manager.

6.14 Termination procedures

6.14.1 HR must notify the IT 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 IT Manager.

6.17 Workstation Access Control

6.17.1 All workstations must use an access control system approved by Senqu 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 minimises the opportunity for unauthorised users to assume the privileges of the intended user during the authorised user's absence.

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

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 Senqu Municipality incurring financial loss as a result of non-compliance, violation and / or disregard of this policy, Senqu 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 Senqu 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.

Resolution: 019/OCM/17	**Approved 28 July 2017**

10. Senqu Municipality Approval and Sign-Off

Date of Approval by Council: 28 July 2017
Resolution Number: 019/OCM/17

_____ _____

MM YAWA **DATE**
MUNICIPAL MANAGER

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.

Resolution: 019/OCM/17	**Approved 28 July 2017**