IT Operating Systems Security 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

Resolution: 019/OCM/17 Approved 28 July 2017

IT Operating Systems Security Policy

As a government institution, Senqu Municipality must implement an IT Operating Systems Security Policy. Effective implementation of this policy will minimise the risk of unauthorised access to the Municipality's Operating Systems.

Resolution: 019/OCM/17 Approved 28 July 2017

TABLE OF CONTENTS

1. Version Control

Full Title	**Senqu Municipality's IT Operating Systems Security Policy**
Short Title	IT Operating Systems Security Policy
Author(s)	Mr R Johl
Version	0.1

Authors	Mr R Johl
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

2. Definitions

Term	Meaning
IT	Information Technology
ICT	Information and Communication Technology
Municipality, the	Senqu Municipality

3. Introduction

Senqu Municipality requires an IT Operating Systems Security Policy to ensure that consistent security controls are applied to minimise the risk of vulnerabilities on the network.

4. Purpose

This document is to provide guidance for the Information Technology (IT) security controls that should be implemented for Senqu Municipality on the Windows operating system.

5. Scope/Audience

This document outlines the technical security values or parameters that should be implemented on Senqu Municipality's Windows servers.

6. Changes to Operating System

Changes to the Window Operating System should be done in accordance with the Municipality's IT Change Management Policy and Procedures.

7. User Administration Procedures

Refer to the User Access Management Policy for the Registration and Termination of users.

7.1. Accounts with administrator access

The following accounts have Domain Administrator permissions:

- Administrator
- Bothaj
- Daleneo
- Tselei
- Matisoo

7.2. System Accounts

The IT Manager must ensure that password expiry does not apply to system accounts. The accounts should either be renamed or disabled where they are not required.

The following are Senqu Municipality's System Accounts:

Account Name	Comment
Administrator	**Built in account**

7.3. Dormant User Accounts

User accounts need to be reviewed periodically to determine if there are dormant user accounts on Active directory. If discovered, dormant user accounts need to be deactivated unless a valid reason is given to preserve them.

8. Password Policies and Procedures

8.1. Procedures for changing forgotten passwords

Refer to the User Access Management Policy for password reset procedures.

8.2. System Account policy settings

The following account policy settings must be implemented on all Windows servers.

Restriction	Setting
Maximum password age	Expires in 30 Days
Minimum password age	1 day
Minimum password length	At Least 8 Characters
Password history length	Remember 24 Passwords
Account Lockout	Enabled
Lockout accounts after	3 bad attempts
Counter resets after	1440 Minutes
Lockout duration	0 Minutes (Forever)
Password Complexity	Enabled
Password Reverse Encryption	Disabled
Default passwords shipped with operating systems/program products for use during system and product installation/setup	Change as soon as possible
Password Never Expires	May not be enabled for any user ID's
Password Never Expires Exception	Admin Password for all services (AV, Management, Backup etc.)

8.3. Event log security settings

Log	Setting
Application	Enabled
Security	Enabled
System	Enabled

8.4. User IDs

System Value/Parameter	Setting
Required action for: • Creating new user ID's • Password resets	Set an initial password and force the user to change it. The check box 'User must change password at next login' must be selected.
Guest account which allows system login without entry of a specific password	Disable
Administrator account	Rename to a more secure name or have a long complex password with a minimum of 15 characters.

9. Audit Policy Settings, Logging, Reviewing and Follow-up of Security Logs

- The following audit logs must be enabled:

Audit Status	Policy	Success	Failure
Enabled	Audit account logon events		X
Enabled	Audit account management		X
Enabled	Audit directory service access		X
Enabled	Audit logon events		X
Disabled	Audit object access		
Enabled	Audit policy change	X	X
Enabled	Audit privilege use		X
Disabled	Audit process tracking		
Enabled	Audit system events	X	X

10. Business Use Notice

Recommended Setting	Description
Yes	WARNING: This is a Senqu Municipality computer system. This computer system, including all related equipment, networks, and network devices (specifically including Internet and e-mail access), is provided only for authorised municipality use only. Senqu municipality computer systems may be monitored for all lawful purposes, including that their use is authorised, for the management of the system, to facilitate protection against unauthorised access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorised municipal entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorised purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this municipality computer system, authorised or unauthorised, constitutes consent to monitoring of this system. Unauthorised use may subject you to criminal prosecution under the Data Protection Act of South Africa. Evidence of unauthorised use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.

11. Trusted and Trusting Domains

The current domain trusts is:

- **Trust name:** DIRECTION_OUTBOUND TYPE_UPLEVEL

12. Remote Access Services:

Senqu currently allows for remote desktop services via the following static IP's.

IP Address	Server	Port
197.157.223.58	MIS-Server	3389 (Remote Desktop)
197.157.223.59	CW-Server	443 (SSL), 491, 3389 (Remote Desktop)
197.157.223.61	SebSQL	80, 1433, 1434, 3389 (Remote Desktop)

13. Network connections

The below are the buildings connected to the Municipality, and the medium of connectivity.

Building name	Medium of connectivity
Fleet yard	Wireless
Technical corporate services	Fiber
Tourism Office	Wireless
Offsite backups - Lady Grey	UTP cable
Sterkspruit Offices	Wireless
Barkly East Offices	Wireless
Barkly East Traffic Offices	Wireless

14. Network shares

The following shares with the following permissions are available on the network:

Share	Trustee	Authorisation	Description
ADMIN$	No DACL Found	-	Remote Admin
APN	SENQUDOMAIN\tobbenl	Full Control	APN
	SENQUDOMAIN\rothmajam	Full Control	
	SENQUDOMAIN\bothaj	Full Control	
C$	No DACL Found	-	Default share
CertEnroll	\Everyone	Read	Active Directory Certificate Services share
D$	No DACL Found	-	Default share
data$	Everyone - User Specific with all rights as per user	Full Control	data$
F$	No DACL Found	-	Default share
IPC$	No DACL Found	-	Remote IPC
NETLOGON	Everyone – A script maps each to their own data share and to Public		Logon server share
NETLOGON	BUILTIN\Administrators	Full Control	-
Public	\Everyone	Full Control	Public
Public	BUILTIN\Users	Full Control	
SophosEM	\Everyone	Read	SophosEM
SophosUpdate	BUILTIN\Administrators	Full Control	SophosUpdate
SophosUpdate	\Everyone	Read	-
SophosUpdate	SENQUDOMAIN\Administrator	Read	-
SUMInstallSet	Sophos Update Manager Installer	\Everyone	Sophos Update Manager Installer
SYSVOL	\Everyone	Read	Logon server share
SYSVOL	BUILTIN\Administrators	Full Control	Logon server share
SYSVOL	NT AUTHORITY\Authenticated Users	Full Control	Logon server share

15. Patch Management

Workstations and servers owned by the Municipality must have up-to-date operating system security patches installed to protect the assets from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by the Municipality.

15.1 **Servers** - Servers must comply with the minimum baseline requirements that have been approved by IT Management. These minimum baseline requirements define the default operating system level, service pack, hot fix, and patch level required to ensure the security of the asset and the data that resides on the system. Any exception to the policy must be clearly defined and documented.

15.2 **Workstations** - Desktops and laptops must have automatic updates enabled for operating system patches and virus definitions. These updates include Driver updates, Windows updates, OS Security updates, Anti-Virus updates, Back-up Software updates. This is the default configuration for all workstations built by the Municipality. Any exception to the policy must be clearly defined and documented.

The organisation will have a centralised WSUS server. This server will download the patches during the night and upload to workstations during the day.

The organisation will also have a centralised Anti-Virus Package. New virus definitions will be downloaded during the night and uploaded to workstations during the day.

This setup is intended at reducing network bottlenecks.

16. Policy Violations

16.1 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.

17. Policy Review

17.1 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.

18. Publishing the policy

18.1 The policy shall be made available and accessible to all employees through manuals/hard copies.

19. 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 Operating Systems Security Policy as part of the ICT Corporate Governance Framework be approved by Council.