SENQU

MUNICIPALITY

IT Risk 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 Risk Management Policy

As a government institution, Senqu Municipality must implement and support risk management relating to information systems. This includes reducing IT-related risk as well as integrating the management of IT-related risk with the Municipality's overall risk management strategy.

Table of Contents

1. Version Control

Full Title	Senqu Municipality’s IT Risk Management Policy
Short Title	IT Risk Management Policy
Author(s)	Mr N Suleman
Version	0.1

Authors	Mr N Suleman
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
Municipality, the	Senqu Municipality
IT	Information Technology

3. Introduction

As a government institution, Senqu Municipality must implement and support risk management relating to information systems. This includes reducing IT-related risk as well as integrating the management of IT-related risk with the Municipality's overall risk management strategy.

4. Purpose

The purpose of this policy is to ensure that all IT risks are effectively and efficiently managed.

5. Scope/Audience

This policy applies to all employees of Senqu Municipality and all parties that interact with the information and systems of the Municipality.

6. Roles and Responsibilities

The table below describes the key stakeholders and their respective roles and responsibilities in terms of IT Risk Management.

Table 1: Roles and Responsibilities

Role	Responsibilities
IT Manager	The IT Manager must ensure that effective IT Risk Management is established within the Municipality.
Directors and Managers	Risk management is a key responsibility of management. To achieve its business objectives, management must ensure that sound risk management processes are in place and functioning. Directors and Managers have overall responsibility for managing risks related to municipal objectives and risk management.
Audit and Performance Committee	The Audit and Performance Committee has an oversight role to determine that appropriate risk management processes are in place and that these processes are adequate and effective.
Municipal Manager	The Municipal Manager must ensure the establishment and maintenance of effective, efficient and transparent systems of financial and risk management and internal control.

7. Risk Management Evaluation

7.1 The level of IT-related risk that the municipality is willing to accept in pursuit of its objectives (risk appetite) must be determined.

7.2 IT risk tolerance thresholds must be evaluated and approved based on the municipality's acceptable risk and opportunity levels.

7.3 The IT environment must be subject to risk assessments and evaluation to ensure compliance with national standards and legislation.

8. Risk Identification

8.1 Risk data relating to IT risks of the Municipality's internal and external operating environment must be recorded. These internal and external factors may include:

Table 2: External Factors

External Factors	
Economic and Business	Related risks might include emerging or movements in the international, national, provincial markets and globalisation.
Natural Environment	Risks might include such natural disasters as flood, fire or earthquake and sustainable development.
Political	Risks might include newly elected government officials, political agendas and new legislation and regulations. The impact of labour unrest and service delivery protests.
Social	Risks might include changing demographics, shifting of family structures, work/life priorities, social trends and the level of citizen engagement.
Technological	Risks might include evolving electronic commerce, expanded availability of data and reductions in infrastructure costs.

Table 3: Internal Factors

Internal Factors	
Infrastructure	Risks might include unexpected repair costs or equipment incapable of supporting production demand.
Human resource	Risks might include increase in number of on-the-job accidents, increased human error or propensity for fraudulent behavior.
Process	Risks might include product quality deficiencies, unexpected downtime or service delays.
Technology	Risks might include inability to maintain adequate uptime, handle increased volumes, deliver requisite data integrity or incorporate needed system modifications.
Governance and Accountability Frameworks	Values and ethics, transparency, policies, procedures and processes.

8.2 Periodic IT risk assessments must be performed to identify new or emerging risk issues and to gain an understanding of the internal and external risk factors.

9. Establishment of Risk Management

9.1 The municipality must implement appropriate measures to identify and respond to changing and new risks.

9.2 The municipality must take appropriate steps to proactively identify IT risk, opportunity and potential business impacts.

9.3 Risk communication plans and risk action plans must be developed to cover all relevant business units.

9.4 Changing and new risks must be promptly responded to, reported to the appropriate levels of management and, where necessary, discussed during the IT Steering Committee or Audit and Performance Committee meetings.

9.5 The approach, capturing and reporting of measurement activities against goals/metrics must be approved.

9.6 The key goals and metrics must be identified for the governance and management processes that are included in the risk assessment.

10. Risk Assessments

10.1 IT Risk Assessments must take place at least on an annual basis.

10.2 IT Risk Assessments must be conducted on the IT environment according to the risk management policy adopted by the Municipality.

11. IT Risk Register and Reporting

11.1 A risk register of IT risks must be maintained and updated with results from risk assessments.

11.2 The IT risk register must be updated when an IT Risk Assessment is performed.

11.3 The following minimum information is to be maintained and recorded in the IT risk register:

11.3.1 Priority

11.3.2 Risk Name

11.3.3 Risk Description

11.3.4 Risk Category

11.3.5 Causes

11.3.6 Risk Owner

11.3.7 Existing Controls

11.3.8 Control Strength

11.3.9 Desired Control Strengths

11.3.10 Risk Improvement Plan

11.3.11 Risk Improvement Plan Owner

11.3.12 Target Date

11.3.13 Risk Improvement Plan Progress

11.4 The detail contained in the IT risk register must be used as the reporting tool to view and track the state of IT risk management within the Municipality.

11.5 The IT risk register will be maintained by the IT Manager

11.6 The following table contains the risk register* work sheet meanings:

IT Risk Register Work sheets	Meanings
Risk Register – Main	All Risks need to be captured into this worksheet.
Risk Register – Top 15	Contains the top 15 IT Risks (automatically populated).
Risk Metrics	Measures and explanations of IT Risks.
Graphs – Inherent	The risk that an activity would pose if no controls or other mitigating factors were in place. (risk before controls) (automatically populated).
Graphs – Residual	The risk that remains after controls are taken into account (the risk after controls). (automatically populated).

*The Standard Senqu Risk Register

12. Monitoring of Risk Management

12.1 The risk register must be monitored to determine the extent of it being managed within the municipality's risk appetite threshold.

12.2 Key goals and metrics of risk governance and management processes must be monitored against targets to identify deviations and requirements for remedial actions.

12.3 Key management must be able to review the municipality's progress towards achieving IT risk management goals.

12.4 Risk management issues must be reported to the Audit and Performance Committee and/or the Municipal Manager where necessary.

13. Responding to Risk Events

13.1 Risk events are events that can potentially have a negative impact on the Municipality's IT environment, which could lead to inefficiencies or potential monetary/data losses. Risk events can be categorised as recurring events or non-recurring events.

13.2 The following responses can be taken for IT Risk events:

13.2.1 Risk Avoidance: A decision not to be involved with a risk situation. The decision will be not to proceed with a particular activity or project because upon assessment, the activity represents such a great risk that there is limited ability to control the risk and that there is little benefit in pursuing the activity;

13.2.2 Risk Control: Is the pro-active control of adverse consequences of a risk by implementing preventative measures. It is the risk, which is cost effective to control or treat;

13.2.3 Risk Transfer/Sharing: It is the risk that upon assessment shall be considered cost effective to transfer to third parties or otherwise sharing a portion of the risk with the third party; and

13.2.4 Risk Retention: It is the risk that upon assessment shall be considered cost effective to be accepted or tolerated due to its limited impact on the Municipality.

13.3 A cost-benefit analysis of potential risk response options must be performed for the optimal response actions to be selected.

13.4 In determining the appropriate responses, management must consider:

13.4.1 Evaluating the effectiveness of current measures in place to reduce the risk to an acceptable level; and

13.4.2 Considering the control measures of leading practices and those implemented by other government institutions, Municipalities or local authorities that could be used to mitigate the risk more effectively.

13.5 A high-level plan must be documented to implement key controls to mitigate identified risks.

13.6 Controls that must be selected may include both Technical controls (access control systems, firewalls, etc) and Non-Technical controls (policies and procedures etc).

14. Policy Violations

14.1 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.

15. Policy Review

15.1 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.

16. Publishing the Policy

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

17. 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 Risk Management Policy as part of the ICT Corporate Governance Framework be approved by Council.