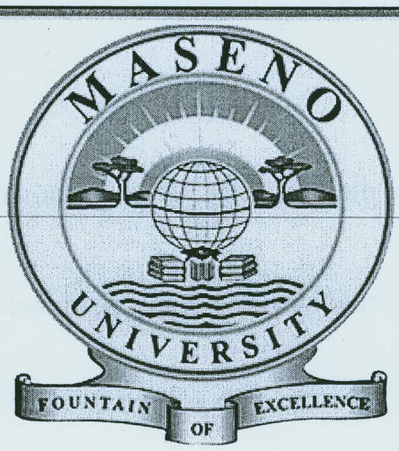

MASENO UNIVERSITY

RISK MANAGEMENT POLICY FRAMEWORK

FEBRUARY, 2017

VISION

The University of Excellence in discovery and dissemination of knowledge.

MISSION

To discover, harness, apply, disseminate and preserve knowledge for good of humanity.

CORE VALUES

National Interest

The University shall promote national interest in all its undertakings

Relevance

The University is committed to ensuring relevance in its programs and activities.

Excellence

Excellence shall be targeted in outputs of the university.

Equity

The University shall ensure that there is equity in all the opportunities within its jurisdiction.

Quality

All outputs and processes of the University shall ensure that quality is maintained.

Integrity

The University shall ensure integrity in all their undertaking.

PREAMBLE

Maseno University is a Public University established under the provisions of Universities Act 2012 and through the Maseno University Charter 2013. Further, the University is governed by Maseno University Statutes 2013 having drawn from all relevant laws.

The current economic trends emerging in both external and internal environments calls for team approach, user friendly and objective oriented systems of operations. When financial and other institutional functions run smoothly, it is often assumed that it will always be so without much thought about the risks involved.

Leading institutions and governments place the issue of risk management very high in their priority list as it plays a significant role in key decision making process. It is in view of this that the Ministry of Finance issued a Treasury Circular No. 3 of 2009 on risk management in which all government entities and state corporations were required to develop and implement institutional risk management policy frameworks.

Maseno University has developed this framework as an integral part of good management practice and is a significant internal control tool which will ensure that the board of management identifies measures and effectively manages its risks in order to meet both operational and strategic objectives it has designed to achieve.

Prof. Julius Omondi Nyabundi PhD, OGW
VICE-CHANCELLOR
MASENO UNIVERSITY

TITLE, APPROVAL AND COMMENCEMENT

This Policy shall be known as the Risk Management Policy Framework for Maseno University. The Policy has been developed in accordance with all relevant legislations.

The Policy development and approval process has been fully executed in accordance with Section 18 (9, 11) of the Universities Act 2012, Section 19(2) (q) of Maseno University Charter 2013 and Schedule 1(12) (q) of Maseno University Statute 2013. It was duly approved at the ..Council meeting.....held on 28th Feb. 2017.

The Policy shall take effect from the date of its approval herein above.

APPROVED BY:

..... **DATE:** 28th Feb. 2017

PROF. ROSALIND MUTUA PhD

CHAIRMAN OF COUNCIL

TABLE OF CONTENT

DEFINITION OF TERMS

The terms applied in this Policy will carry the interpretation in the primary acts as well as other acts of general references in its development. Notwithstanding these provisions, the following interpretations shall apply as hereunder:

"Communication and consultation" is the continual and interactive process that the organization conducts to provide share or obtain information and engage in dialogue with stakeholders regarding the management of risk.

"Controls" are the measures that are modifying risks. Controls include any process, policy, device, practices or other actions that act to minimize negative risks or contain them to an acceptable level.

"Operational risk" is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

"Residual Risk" is the risk remaining after risk treatment/application of controls.

"Risk" is the effect of uncertainty on objectives. A risk is often specified in terms of an event or circumstance and the impacts that may flow from it.

"**Risk Champions**" these are existing members of senior management (not exclusively) charged with the responsibility to support the risk management process within their specific allocated functions.

"Risk Appetite" is the University approach to assess and eventually pursue, retain, take or turn away from risk

"Risk Assessment" refers to the overall process of identifying, analyzing, and evaluating risks. It may also be referred to as 'risk profiling' and may involve a qualitative and/or quantitative assessment.

"**Risk Aversion**" is a manifestation of people's general preference for certainty over uncertainty and for minimizing the magnitude of the worse possible outcome to which they are exposed.

"Risk Attitude" refers to the University's approach to assess and eventually pursue, retain, take or turn away from risk.

"Risk identification" refers to the process of finding, recognizing and describing risks.

"Risk Management" coordinated activities to direct and control an organization with regard to risk.

"Risk Management Framework" is the set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.

"Risk Owner" is the person or entity with the accountability and authority to manage a risk.

"Risk Profiling" is a structured approach to the identification and assessment of risk. The output of the risk identification and assessment process is a completed risk profile (or Risk Register).

"Risk Register" is a documented record of each risk identified. It specifies a description of the risk, its causes and its impacts, a list of current controls, any further actions that are planned, a due date for each action, an assessment of the impact and the likelihood of the risk occurring, and a risk rating.

"Risk Treatment" is a process to modify risk. Risk treatments that deal with negative impacts are sometimes referred to as 'risk mitigation' and can involve avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk or transferring the risk to others or insurance.

"Risk Tolerance" is the amount of risk that the university is comfortable taking or the degree of uncertainty that the University is able to handle.

1.0 POLICY STATEMENT

Maseno University is committed to managing its risks to an acceptable level in all areas of its operations. The Risk Management Policy Framework will therefore be applicable at both corporate and operational level, its applicability will be extended to external strategic risks arising from environmental, technology, legal and regulatory framework. It shall form an integral part in planning and reporting, and will ensure a structured approach is followed to ensure fundamental risks are mitigated.

2.0 OBJECTIVES OF THE POLICY

The objectives of University Risk Management are to help the University make informed choices which include:-

i. Improve the University's performance by informing and improving decision making and planning by maximizing opportunities and minimizing adversities.
ii. Factor in all the risks when making strategic, management and operational decisions.
iii. Promote a more innovative, less risk averse culture in which taking of calculated risks in pursuit of opportunities to benefit the University is encouraged.
iv. Provide a sound basis for integrated risk management and internal control as components of good corporate governance.
v. Aligning and integrating risk management processes and internal controls with University's functions and income generating activities.

3.0 BENEFITS DERIVED FROM THE POLICY

Upon effective implementation of this policy, the University stands to: -

i. Increase the likelihood of achieving the University's aims, objectives and priorities.
ii. Prioritize the allocation and utilization of resources enabling the University management to direct greater focus on the issues that really matter.
iii. Give an early warning to potential problems which prevent risks and legal liabilities resulting into fewer surprises or crisis.

iv. Provide staff with skills and improved understanding of the key risks and their wider implications to be confident risk takers.

v. Promote risk identification, mapping and management.

vi. Help in the enforcement and compliance with statutory laws, regulations and guidelines.

4.0 SCOPE OF THE POLICY

The application of this policy integrates both the extent and the depth of its use for the benefits of the university. In this regard: -

i. The policy shall be applied to all operational aspects of the university, and shall consider external strategic risks arising from related legal and regulatory requirements, as well as wholly internal risks.

ii. The University's risk management approach shall be forward looking. It will not only focus on risks and how to mitigate them, but also to explore and exploit available opportunities and capitalize on the University's corporate strength.

iii. Articulate and communicate the objectives of the University.

iv. Determine the university's risk appetite.

v. Establish an appropriate internal environment.

vi. Identify potential threats to the achievement of the objectives.

vii. Assess the risks and regularly mapping the same complete with responsive interventions (i.e. impact and likelihood of the threat occurring)

viii. Select and implementing responses to risks.

ix. Undertaking control and other response activities.

x. Communicating information on risks in a consistent manner at all levels in the university.

xi. Centrally monitoring and coordinating the risk management process.

xii. Providing assurance with which risks are managed.

5.0 GENERAL PRINCIPLES OF THE RISK MANAGEMENT POLICY

The University shall organize and conduct its risk management responsibilities upon guidance by general principles including but not limited to: -

i. All risk management activities shall be aligned to the University's core mandates, visions, missions, objectives and priorities. It is designed to protect and enhance the reputation and standing of the University in the higher education sector.

ii. Risk Analysis shall form part of the University's strategic planning, operational planning and investment/project appraisal procedures,

iii. Risk Management shall be based on internal controls which are embedded in the day to day operations of the University.

iv. The University's Risk Management approach shall inform and direct both strategic and tactical activities to gain an assurance on the reliability of the University's systems, and shall form the key means by which the Council gains direct assurance.

6.0 RISK MANAGEMENT POLICY METHODS

In standardizing its approach to risk management and enhancing effectiveness thereto, a multilevel approach will be informed by several methods including but not limited to: -

i. Risk Management in the University shall adopt proactive and reasoned approach; strategic and operational risks shall be identified, objectively assessed and actively managed.

ii. The aim shall be to anticipate and where possible avoid risks rather than dealing with their consequences. However, for some key areas where the likelihood of the risks occurring is relatively small but the impact on the university functions may be enormous, contingency plans shall be developed to deal with the effect.

iii. In determining an appropriate response, the cost of control/risk management and the impact of the risk occurring shall be balanced with the benefits of reducing the risks, through cost benefit analysis.

iv. Some risks shall be managed by transferring them to third parties e.g. performance bonds, Insurance, guarantees and contracts etc. other risky ventures will be terminated, while others with low impact will be accepted,

outsourcing of services may be an option, a decision which shall be arrived at through cost benefit analysis.

v. Diversification through effective and efficient investment portfolio management shall be strictly observed, through the guidance of the Council and University Board of Management.

vi. Automation of services through innovation technology and practices.

vii. All members of the University management have a responsibility for maintaining good internal controls and managing risks in order to achieve personal, team, and corporate, objectives. Collectively, the management board shall have the appropriate knowledge, skills, information and authority to establish, operate and monitor the system of internal control. The Board of Management shall therefore acquire an understanding of the university, its objectives, the risks it faces and understand how those risks affect other stakeholders.

viii. Determination and assessment of risks shall be through methods that include: -

a. By statistical methods e.g. trend analysis, variance analysis
b. Interviewing
c. Risk Workshops
d. Review of financial statements
e. Auditing
f. Document analysis
g. Assessment of risk tolerance level
h. Any other

ix. The acceptable risk tolerance levels shall be reviewed and approved by Council.

7.0 AREAS OF POTENTIAL RISKS

i. **Human Resource Management and Development:** – recruitment, training, promotion, career development, payroll management etc.

ii. **Financial Management:** – cash management, record keeping, revenue and expenditure, supervision and oversight, imprests, travelling and accommodation, payment management, fees and other charges, exchange rate fluctuations, interest rate fluctuations etc.

iii. **Technology:** - access to stored information, management of records, use of stored information, security installations and management.

iv. **Registry:** - access to registry files, management of registry files, security and storage of registry files etc.

v. **Supplies and procurement:** - tenders and tender documents, storage and management of goods and services, contracts and contract management, goods and service orders management, market analysis and value for money management, acquisition and disposal of assets, management of University assets e.g. motor vehicles, telephones, personnel, computers, stationary etc.

vi. **Policy and governance:** - policy formulation and implementation, compliance and enforcement of laws, regulations and standards, conduct of business of governance of Council and Management, implementation of resolutions, management of records on policy and governance etc.

vii. **Academic and students affairs:** - admissions, teaching, examinations, quality assurance, curriculum development and approval, certification, students affairs management etc.

viii. **Intellectual property rights:** patent and copyrights

ix. **Environmental and Social risk:-** Ethnic problem, infrastructure, security e.t.c

8.0 ROLES AND RESPONSIBILTIES

Risk management is the responsibility of all staff at Maseno University. Management Board of the University is responsible for the development of the Risk Management Policy Framework and ensures its implementation as an effective tool for risk mitigation arrangements. Management board shall therefore ensure risk management processes are integrated with other planning processes and management activities.

8.1 Engagement and role of Staff

Engagement of all staff in the risk management process is mandatory. Staff more directly involved in the risk management process by virtue of their job responsibilities will have personal responsibilities which include completing the annual risk matrices reports

indicating that identified risks for which they are assigned as owners have been addressed, monitored and controlled.

8.2 The Heads of Divisions and Departments

i. Establish and maintain a risk data base for all significant risks identified in their divisions.
ii. Continuously update The Risk Data Base.
iii. Maintain a risk profile which is prioritized in terms of impact and likelihood
iv. Maintain a risk management action plan and contingency plans
v. Maintain evidence of meetings to regularly review and monitor the risk profile, action plan and contingency plans.
vi. Comply with university's policies and guidance manuals.
vii. Monitor risks on a daily basis. It is mandatory for the university to develop structured ways of ensuring key risks are identified, assessed and well monitored by appointing risk champions. Risk champions shall:-
    a. Escalate instances' where the risk management efforts are stifled, such as on individuals try to block risk management initiatives.
    b. Adds value to risk management process by providing guidance and support to manage "problematic risks and risks of a transversal nature."
    c. Register changes to risk registers.
    d. React to early warning indicators
viii. Review implementation of risk responses

8.3 Internal Audit

The role of internal audit is to provide independent objective assurance that the University risks are being mitigated to an acceptable level and report where they are not. Internal audit shall assist the university management in their assessment of the effectiveness of internal controls over financial transactions processing and reporting

8.4 Audit and Risk Management Committee of council.

Among the terms of reference spelt out in Maseno University Statutes 2013, Audit and Risk Management Committee shall:-

i. Receive, review and recommend internal control mechanisms towards improving efficiency, effectiveness, transparency and accountability.
ii. Review and submit to Council the Audit and Risk Management Committee charters and the internal audit work plans.
iii. Review and submit proposals to council on improvements of efficiency and effectiveness of management systems including and not limited to high risk areas such as public finance, human resource, academic programmes and general internal controls.
iv. Review and submit to council reports on compliance with policies, laws, regulations, procedures, plans and ethics.
v. Initiate special investigations/audit on allegations, concerns and complaints regarding corruption, lack of accountability and transparency among others.

8.5 University Council

The Council approves the policies of the University and provides the overall oversight authority accorded by Maseno University Statutes 2013. It is the responsibility of the Council to approve the Risk Management Policy Framework and ensure its implementation. The Council shall act on Audit and Risk Management Committee reports. It shall set the tone and influence the culture of risk management at the University.

9.0 RISK MANAGEMENT PROCESS

This Risk Management Policy Framework provides a comprehensive approach to risk management. Management board of the university owns the risks. It is therefore their responsibility to control, and manage them. The framework recognizes that:-

i. Risks hinder attainment of organizational objectives.
ii. Internal controls mitigate risks.
iii. Internal audit provides assurance that internal controls put in place by management board mitigate identified risks to acceptable levels.

Risk management process spearheaded by Risk Champions shall flow in the following steps;-

i. Risk identification
ii. Risk assessment (evaluation)
iii. Risk ranking (prioritizing)
iv. Risk mitigation, treatment and controlling.
v. Risk reporting and communication
vi. Risk monitoring.

The steps of risk management procedures provide a framework for managing risks as they arise. Sufficient documentation at all levels of the risk management process including explanations and evaluations that facilitate understanding the nature of risks by third parties shall be established.

9.1 Risk Identification

The process of determining what might happen that could negatively affect the achievement of the objectives, why and how it could happen.

9.2 Risk Assessment

Involves amongst others: -

i. An assessment of possible threat.
ii. Possible impacts of the threats.
iii. Likelihood of the threat to occur.

9.2.1 Risk Measurement and classification

	IMPACT	LIKELIHOOD	MEASURE
R I S	Prevent the university from achieving major parts of its objectives for a long time	Almost certain	High
	Prevent the university achieving its objectives for a limited period	Possible	Medium
	Cause minor	Unlikely	low

K	inconvenience not affecting the		
	achievement of objectives.		

9.3 Prioritizing Risk

Risks shall be ranked on the basis of their likelihood and impact. This will determine the mitigation measures applicable as well as assisting in the allocation of resources to mitigate the risks more efficiently and effectively.

Risk criteria

	Impact	**Likelihood**
R	Insignificant	Rare
I	Minor	Unlikely
S	Moderate	Possible
K	Major	Likely
	Catastrophic	Certain

9.4 Risk Mitigation, Treatment and Control.

9.4.1 Risk Mitigation.

After risks have been identified, analyzed, reported and prioritized, an appropriate risk action plan shall be prepared. The current controls designed to address the problems will have to be considered while developing the steps to be taken to manage or contain the risks to acceptable levels. A timetable for action shall be prepared and the names of the risk owners and action officers shall be charged with implementing agreed action plans.

9.4.2 Risk Treatment

This is the process that modifies risk. Risk treatments that deal with negative impacts are sometimes referred to as 'risk mitigation' and can involve avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk or transferring the risk to others or insurance.

9.5 Risk Reporting and Communication.

Identified, assessed and mitigated risks shall be communicated so that knowledge is shared across the University. Every risk champion shall report fortnightly and on ad hoc basis.

The reporting of risks ensures:-

i. There is appropriate sharing of risk intelligence across the University.
ii. The Management Board obtains the relevant information on the risk universe and designs ways of responding to them.
iii. The whole University community is sensitized on the risks profile; risk ranking and understanding of risks is enhanced.

Risk report will include the following tools:-

i. Risk logs (risk register)
ii. Annual risk matrix (risk inventory) with action plan.
iii. Quarterly risk map
iv. Incidental Adhoc reporting
v. Whistle blower program.

9.5.1 Risk register

The Risk Champion will keep an up to date record of all the risks identified (risk universe) and the details of how they have been dispensed with the Management Board, Audit and Risk Management Committees and other senior managers of the University.

9.5.2 Annual risk matrix

Every department of the University shall prepare the annual risk matrix and forward the same to the Risk Champion who will review them with the risk owners. The combined departmental self-assessment and any other risks identified will form the annual risk matrix for the University. The annual risk matrix will contain an action plan with an allocation of responsibility for risk mitigation and time frame.

Follow up of action plans shall be part of quarterly review process. Newly detected risks shall be added while risks no longer applicable shall be deleted.

9.5.3 Quarterly risk maps

The Risk Champion shall follow up on major risks from the risk map and ensure action plan is being implemented as expected. Major risks which arise shall be reported within Ad hoc reports. The quarterly risk map report shall be sent to the Audit and Risk Management Committees with appropriate comments from the Risk Champion.

9.5.4 Ad hoc reporting of newly recognized major risks

Heads of departments shall report newly recognized risks to the Risk Champion. Ad hoc reports shall be used to highlight emerging risks that have not been identified in the past and on any unresolved risk issues, it shall be the role of risk owners i.e. departmental heads and Risk Champion to regularly review progress on achievement against action plan.

9.5.5 Whistle blower program

The University shall strengthen its approach to risk identification, monitoring and mitigating fraud and corruption by developing a whistle blower program. This will provide a platform for anonymous reporting of incidents by members of the public, members of staff and other stakeholders. To facilitate this, Management Board shall provide suggestion boxes in all departments which shall be supplemented by a hotline to a member sitting in the Audit and Risk Management Committee. The whistle blower program shall ensure high risk incidents are promptly brought to the attention of the top management and ensure all information providers are accorded the confidentiality needed to encourage participation.

9.6 Risk Monitoring

In this section, complete risk mitigating actions are monitored for effectiveness and to make sure that they have not caused any knock-on effects. The Risk Owner should determine this through their monitoring. If the risk has increased, further controls may be necessary or, if the risk is outside the University's control and deemed too risky, the University may need to withdraw from the activity altogether.

10.0 IMPLEMENTATION

The implementation shall be immediately following the approval of the policy by the relevant structures in line with the implementation plan that will be developed by the Internal Audit Unit.

11.0 POLICY MONITORING

Monitoring of this policy shall be vested in the office of the Internal Audit, the Risk Champions and the Council.

12.0 CUSTODIAN

The Head of Internal Audit unit shall be the custodian of this Policy.

13.0 REVISION AND RESPONSIBILITY

The Policy shall be reviewed after every two years to ensure alignment and relevance to any significant changes in the professional, regulatory, governance and any other environments that affect functionality of risk management processes. The University Management and Council shall be responsible for carrying out the policy review which in turn will input into its revision.