004

KISIINATIONAL POLYTECHNIC

RISK MANAGEMENT POLICY

KNP /RMP/18

FirstEdition 2020

KISII NATIONAL POLYTECHNIC

RISK MANAGEMENT POLICY		**Policy No.** KNP /RMP/18
Principal's Signature		Date 6/5/2021
Approval by Governing Council Chairman's Signature		Date 6/5/2021
Responsible Office	MANAGEMENT REPRESENTATIVE	

Table of Contents

1.0 HISTORICAL BACKGROUND

Kisii National Polytechnic was founded in 1971 as a Harambee Institute of Technology. It was registered in 1972 under the Education Act. CAP 212 of the laws of Kenya with the objective of providing technical education and training for youths. It was moved from St. Vincent Centre where it was initially housed, to the current site in 1980. The first buildings to be put up were Woodwork Technology and Mechanical Engineering workshops, Typing Pool, Hostels, Kitchen and Dining hall. The curriculum then was Secretarial and Building technology. The institute was elevated to a national polytechnic in May 2016 through Legal notice No. 93. Since then more courses have been introduced and currently Kisii National Polytechnic offers more than eighty-eight (88) courses in Certificate and Diploma levels.

Science and Technology (S&T) activities have been recognized in the institution since its inception as vital to social and economic development. There has been rapid expansion of Science and Technology since the enactment of Science and Technology Act CAP 250 of the laws of Kenya (1977).

The college is managed by the Governing council and college administration comprising of the Principal, Deputy Principals, the Registrar, the Dean of Students, Heads of Departments and their Deputies. Day to day learning activities in the college is managed by the Departments.

1.1 VISION, MISSION AND CORE VALUES

1. Vision

"To be the preferred training institution for technical and vocational skills development"

2. Mission

To develop highly qualified, globally competitive and innovative human resource by `providing quality Training, applied Research & extension and Entrepreneurship skills that are responsive to market demands.

3. Core values

1. Professionalism and Excellence
2. Creativity and Innovativeness
3. Team work
4. Integrity
5. Accountability and Transparency

1.2 MANDATE

The mandate of the polytechnic is to develop an institution with excellence in training, scholarship, entrepreneurship, research, consultancy, community service and products with emphasis on technology, its development, impact and application within and outside Kenya.

2.0 PURPOSE

The purpose of this policy is to guide the management on identified risks at management and functional levels in KNP.

3.0 SCOPE

This policy applies to all processes in KNP as well as issues related to interested parties

4.0 OBJECTIVES

i. To identify risks associated with KNP processes
ii. To establish appropriate controls to address the risks
iii. To monitor inherent risks within KNP
iv. To review the risk management process for continual improvement

5.0 DEFINITION OF TERMS

i. **Control:** Any measure that modifies a risk.
ii. **Impacts:** The consequences/outcomes of an event affecting an objective.
iii. **Levels of risks:** Magnitudes of risks expressed in terms of combination of consequences and their likelihood.
iv. **Likelihood:** The chance of something happening.
v. **Risks:** Effects of uncertainty to realization of objectives.
vi. **Risk identification:** The process of determining incidences/events that could potentially prevent hinder/derail the achievement of the objectives of the institution.

6.0 INTRODUCTION

KNP shall use a Risk Management process which provides systematic, coordinated and continuous mechanisms to identify, analyze, respond to, monitor and report risks.
The Governing Council is cognizant of the fact that all risks cannot be eliminated completely. However, the Institution shall endeavor, as much as possible within the available resources, to manage risks to acceptable levels in all its activities.
KNP is committed to embedding risk management principles and practices into:

1. strategic and operational plans
2. decision making processes
3. business and financial processes
4. major projects undertaken
5. major transactions entered into with interested parties.

Risk management is based on the proposition that it must add value to the institution - the benefit of reducing risk must be greater than the cost of its management.

7.0 Policy Statements

i. Risk Management is everybody's responsibility, from the Governing Council to individual employees.
ii. Each process owner shall undertake risk assessments and treatment termly or as may be determined by the Audit & Risk Committee of the Governing Council.
iii. Top Management shall ensure that appropriate risk responses are instituted to mitigate the identified risks to acceptable levels.
iv. KNP risk policies, procedures and processes will be consistent with this framework.
v. Risk Management framework shall be communicated and sensitization carried out to all employees of KNP.

vi. Risk management shall be embedded in KNP operations and shall be reviewed for adequacy, suitability and its effectiveness as need arises.

8.0 Risk Management Framework

The Institution shall put in place systems through which risks will be identified, analyzed, mitigated, monitored and reported.

8.1 KNP Risk Management Process

Risks shall be classified as follows:

General risks: risks that can generally affect implementation of the Integrated Management System (IMS) as whole and other operational activities for the institution as defined in clause 6.1.1 of IMS standards.

Information security risks: risks that can affect information and assets of the institution leading to the loss of preservation of CIA as per ISO/IEC27001:2013 clause 6.1.2.

KNP shall adopt a Risk Management process with the following key steps:

1. Risk identification
2. Risk Analysis
3. Risk Response (evaluation and treatment)
4. Risk Monitoring
5. Risk Management Reporting

8.2 Risk identification

Risks will be identified from operational areas or identified processes at functional levels. Information security risks will be determined through identification of risks that can affect information assets.

8.3 Risk Analysis

i. The identified risks will be analysed using KNP Likelihood and Impact Matrix (Refer IMS Manual Appendix).
ii. The KNP Likelihood and Impact Matrix adopt a 3x3 measure in terms of likelihood and impact.
iii. Risk value is a function of likelihood and impact.

8.4 Risk Evaluation

i. Risk levels will be determined by comparison of risk values from risk analysis with the acceptance criteria.

ii. Risks shall be prioritized based on the area of impact and the severity as follows:
   a. Financial impact-priority 1
   b. Loss of information- priority 1
   c. Interruption to routine operation- priority 1
   d. Risks that can be solved by routine operation- priority 1
   e. Welfare and safety- priority 1
   f. Compliance to the legal requirement- priority 1
   g. Damage to reputation- priority 2

   Note:Refer to impact criteria document on IMS manual Appendix

iii. Prioritized risks will be indicated with a prefix P and value of priority e.g. P1,P2 etc.

8.5 Risk Treatment:

i. Risk treatment is the activity of selecting and implementing appropriate control measures to modify the risk.

ii. Risks ranked 'High' must be reported immediately to Top Management and require detailed treatment plans to reduce the risk to acceptable levels e.g. Low.

iii. Risks Treatment option shall be selected from the organization risks treatment adapted option table.

iv. Necessary Controls shall be determined to implement the risk treatment option(s) chosen in (iii) above;

   Note: For IS risks,determined controls in **(iv)** above shall be compared with those defined on Annex A and verify that no necessary controls have been omitted.

v. For IS risks, Statement of applicability (SOA) shall be produced/developed that containsthe necessary controls defined in (IV) and Annex A of ISO/IEC 27001 and justification for inclusions, whether they are implemented or not, and the justification for exclusionsof controls from Annex A;

vi. The RTP shall be documented and communicated to the appropriate risk owners for approval and where applicable for implementation and

vii. Acceptance of residual risks.

viii. Information Security assessments shall be performed termly or when significant changes are proposed or occur.

   Note: Each department shall retain documented information about risks treatment including: risks treatment plan, SOA, treatment options selected etc.

Risks Treatment Options

ACCEPT	A justifiable decision by the risk owner to accept the risk which is within risk acceptable or based on cost benefit analysis.
AVOID	Involves terminating an entire process or part of a process to cushion the organization from the risk. This decision shall be made by top management.
REDUCE	Implementation of risk treatment plan to lower the likelihood and/or the impact.
TRANSFER	The risk is shared to another party that can most effectively manage the particular risk depending on risk evaluation.
TRANSFORM	The risk being transformed from the inherent form to a different form to minimize the risk to acceptable levels.

8.6 Risk Monitoring

KNP shall ensure continuous risk monitoring to give assurance that:

a. risks are managed properly
b. risk response plans remain relevant and cost effective
c. new risk exposures are effectively mitigated
d. resources are efficiently allocated/ re-allocated based on the determined risk profiles.
e. Risks shall be monitored through observations, customer feedbacks, surveys, audits and any other appropriate method. Monitoring will be carried out by use risks assessment tools and treatment plan templates.

8.7 Risk Management Reporting

Risk information shall be communicated both upwards & downwards throughout KNP management structure and to relevant stakeholders.

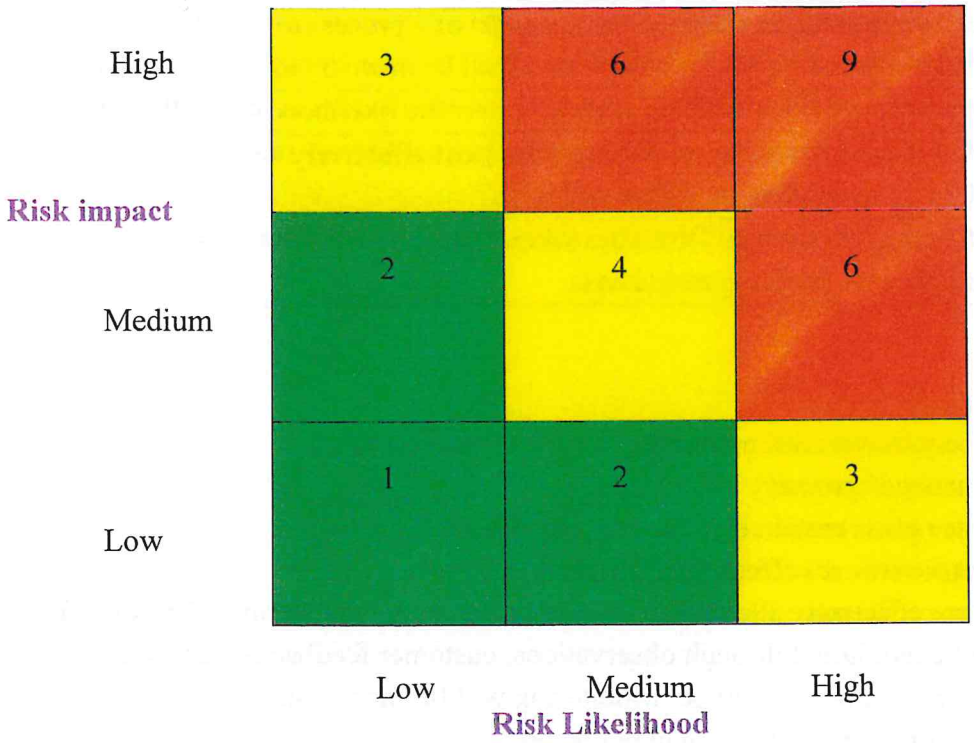
A risk management report shall be done during KNP management review meetings.

9.0 Policy Review

This policy is subject to review every five years or from time to time to incorporate emerging issues. The management will initiate the review and involve all the relevant stakeholders to ensure that the review captures all the emerging issues and relevance is maintained.

10.0 Appendices

APPENDIX I
RISK ASSESSMENT MATRIX



APPENDIX II

RISK ACCEPTANCE