




# KISII NATIONAL POLYTECHNIC

## RISK ASSESSMENT METHODOLOGY

<b>DOC.NO:</b> KNP/ADM/RAM	<b>REV:</b> 0
<b>ISSUED BY:</b> MANAGEMENT REPRESENTATIVE	<b>DATE OF ISSUE:</b>  20 <sup>TH</sup> JANUARY 2021  <b>SIGNATURE:</b>  
<b>AUTHORIZED BY:</b> PRINCIPAL	
<b>ISSUE NO:</b> 01	<b>COPY NO:</b>

**CONTROLLED**

## A. RISK ACCEPTANCE CRITERIA

Impact of Loss ►	LOW	MEDIUM	HIGH
<b>Confidentiality</b>  Ensuring that information is accessible only to those authorized to have access	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
<b>Integrity</b>  Safeguarding the accuracy and completeness of information and processing methods	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
<b>Availability</b>  Ensuring that authorized users have access to information and associated assets when required	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

**CONTROLLED**

## B. RISK ACCEPTANCE CRITERIA

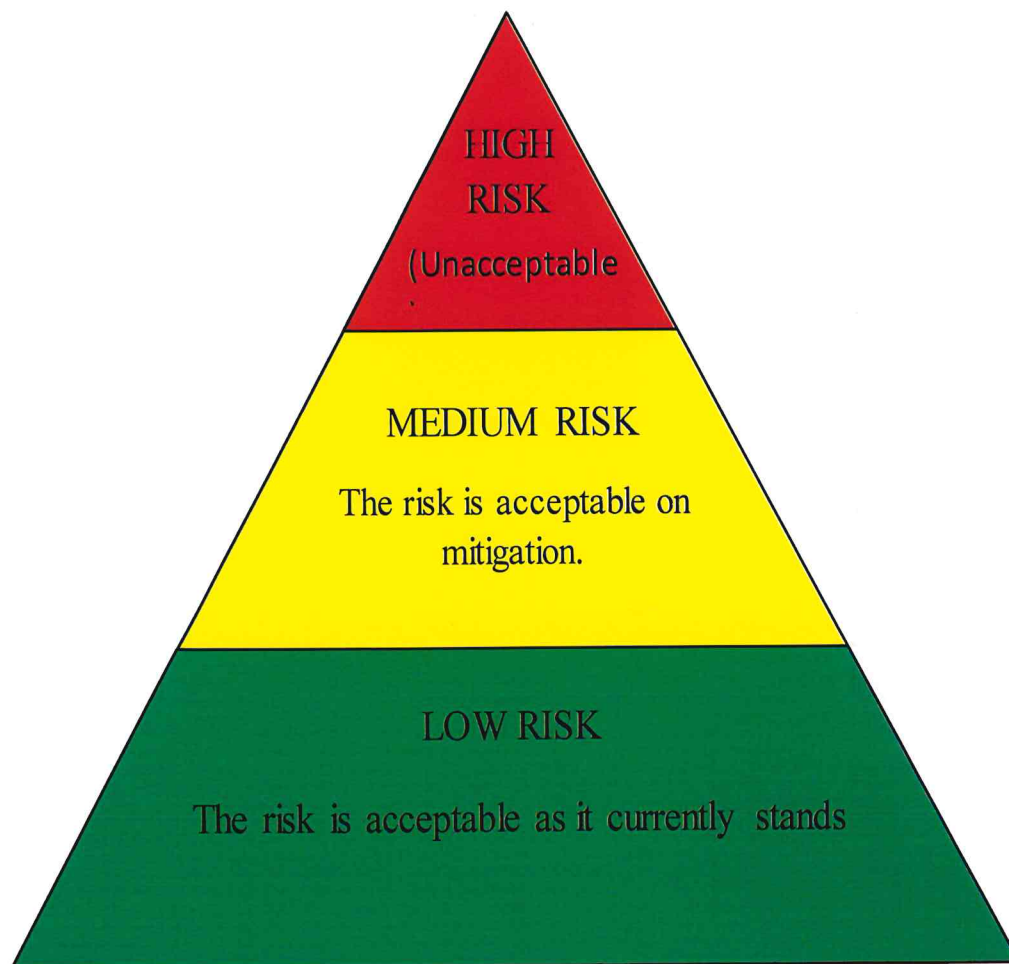
Risk impact	High	3	6	9
	Medium	2	4	6
	Low	1	2	3
		Low	Medium	High
		Risk Likelihood		

**CONTROLLED**

Key:

	High (6 to 9)
	Medium (3 to 4)
	Low (1 to 2)

## C. RISK MATRIX



**CONTROLLED**

#### D. KNP INFORMATION ASSETS REGISTER

Asset Category	Owner	Location
<b>ORGANIZATION</b>		
1. Supplier information	Procurement Officer	Procurement office
2. Press Releases	Principal	Principal's office
3. Partner Information	Principal	Principal's office
4. Risk Assessments –Assets	Management Representative	MR's office
5. Trainee information	Registrar Academics	Registry
<b>ASSET MANAGEMENT</b>		
1. Asset Register	Management Representative	MR's office
<b>HUMAN RESOURCES</b>		
1. Social Security Details	HR	Human Resource Office
2. Personnel Information	HR	Human Resource Office
<b>PHYSICAL &amp; ENVIRONMENTAL</b>		
1. Cell Phones	HR	Human Resource Office
2. Power Supplies	Estates Officer	Estates Office
3. Uninterruptable Power Supplies	ICT Officer	ICT Office
4. Firefighting equipment	Security Officer	Security Office
5. Network Cabling	ICT Officer	ICT Office

6. Equipment maintenance Plans.	Estates Officer	Estates Office
7. CCTV Register	Security Officer	Security Office
<b>COMMUNICATIONS &amp; OPERATIONS</b>		
1. Smart Cards	Registrar Academics	Registry
2. Data Centres	Process Owners	Respective functional levels
3. Computers	ICT Officer	ICT Office
4. Network Devices	ICT Officer	ICT Office
5. Intercom	Deputy Principal Admin	D/P Admin's Office
6. Removable Media	ICT Officer	ICT Office
7. Network Design	ICT Officer	ICT Office
8. Intranet Data	ICT Officer	ICT Office
9. Service Delivery Charter	Principal	Principal's office
<b>ACCESS CONTROL</b>		
1. Active Directory	ICT Officer	ICT Office
2. Domain Name System	ICT Officer	ICT Office
3. Employee Passwords	ICT Officer	ICT Office
4. User Register	ICT Officer	ICT Office
5. Access Rights Register	ICT Officer	ICT Office

**CONTROLLED**

<b>INCIDENT MANAGEMENT</b>		
1. Human Resource Data	HR	Human Resource Office
2. Incident Register	Principal	Principal's office
<b>BUSINESS CONTINUITY</b>		
1. Strategic Plans	Principal	Principal's office
2. Business Continuity Plans	Principal	Principal's office
3. Integrated Management System Manual	Principal	Principal's office
<b>COMPLIANCE</b>		
1. Intellectual Property	Research Development Unit Co-ordinator	Research & Development Office
2. IMS Documentation	MR	MR Office
3. Training Materials	Deputy Principal Academics	Deputy Principal Academics Office

**CONTROLLED**

#### E. RISKS TREATMENT OPTIONS

<b>ACCEPT</b>	A justifiable decision by the risk owner to accept the risk which is within risk acceptable or based on cost benefit analysis.
<b>AVOID</b>	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.
<b>REDUCE</b>	Implementation of risk treatment plan to lower the likelihood and/or the impact.
<b>TRANSFER</b>	The risk is shared to another party that can most effectively manage the particular risk depending on risk evaluation.
<b>TRANSFORM</b>	The risk being transformed from the inherent form to a different form to minimize the risk to acceptable levels.

**CONTROLLED**

## F. KNP RISK ASSESSMENT REGISTER (CORPORATE)

RISK	Risk Identification (Loss of CIA)		L	I	Risk value L x I	Risk Level	Risk Owner
	CIA  Property affected	Cause					
<b>Noncompliance to regulatory and contractual requirements</b>	Regulatory and contractual requirements	Low levels of awareness	1	3	3	Medium	PRINCIPAL
<b>High staff turn-over.</b>	CIA	Search for greener pastures.  Transfer of services	2	2	4	Medium	PRINCIPAL
<b>Political interference.</b>	I	Vested interest(s).	1	2	2	Low	PRINCIPAL
<b>Inadequate funds.</b>	A	Delayed/irregular funding from the government.	2	3	6	High	PRINCIPAL
<b>Access to the network by unauthorized persons.</b>	CI	Hacking,  Disclosure of information or passwords.	1	3	3	Medium	ICT OFFICER
<b>Malfunction of information processing equipment.</b>	A	Virus attack  Malicious damage  Errors in maintenance.	2	3	6	High	ICT OFFICER
<b>Loss of information processing</b>		Theft of equipment.	1	3	3	Medium	SECURITY OFFICER

<b>equipment.</b>	A	Fire.					
<b>Loss of information.</b>	CIA	Fire.  Malicious destruction of records/documents.  Staff turnover.	2	3	6	High	HR OFFICER
<b>Human or natural disasters.</b>	CIA	Epidemics.  Lightning.  Fire.  Vandalism.  Terrorist attacks.	1	3	3	Medium	D/P ADMIN

**CONTROLLED**

### G. KNP CORPORATE RISKS/TREATMENT PLAN

Rank	Risks	Cause	Control Actions	Resources	Treatment Option	Responsibility
1	<b>Inadequate funds.</b>	Delayed/irregular funding from the government.	Plan and seek resources before putting up programmes.	Personnel Funds	Accept	Top management
2	<b>Loss of information.</b>	Fire.  Malicious destruction of records/documents  Staff turnover.	Installing firefighting equipment.  Applying disciplinary measures.  Creating a conducive environment for staff.  Installing fireproof cabinets.  Creating backups.	Funds. Personnel.	Reduce.	Top management
3	<b>Malfunction of information processing equipment.</b>	Virus attack  Malicious damage  Errors in maintenance.	Installing and timely updating the antivirus  Applying disciplinary measures.  Performing preventive maintenance.	Funds Personnel	Reduce	Top management
4	<b>High staff turn-over.</b>	Search for greener pastures.  Transfer of services	Provide incentives  Offer competitive salaries.	Funds. Personnel	Reduce	Top management
5	<b>Noncompliance to regulatory</b>	Low levels of awareness	Regular training and sensitization of staff and relevant	Funds Personnel	Reduce	Top management

	<b>and contractual requirements</b>		stakeholders			ment
<b>6</b>	<b>Access to the network by unauthorized persons.</b>	Hacking,  Disclosure of information or passwords.	Configuring authentication mechanisms	Funds  Personnel	Reduce	Top management
<b>7</b>	<b>Loss of information processing equipment.</b>	Theft of equipment.  Fire.	Securing perimeters.  Labeling of equipment.  Installing firefighting equipment.	Funds  personnel	Reduce	Top management
<b>8</b>	<b>Human or natural disasters.</b>	Epidemics.  Lightning.  Fire.  Vandalism.  Terrorist attacks.	Installing lightning arresters.  Installing firefighting equipment.  Securing perimeters.  Applying disciplinary measures.	Funds.  Personnel.	Reduce.	Top management
<b>9</b>	<b>Political interference.</b>	Vested interest(s).	Control levels of association.	Personnel	Reduce	Top management

**CONTROLLED**