KISII NATIONAL POLYTECHNIC

STATEMENT OF APPLICABILITY

DOC.NO: KNP/ADM/SOA/001	**REV:** 00
ISSUED BY: MANAGEMENT REPRESENTATIVE	**DATE OF ISSUE:** **30th OCTOBER, 2021**
AUTHORIZED BY: PRINCIPAL	**SIGNATURE:**
ISSUE NO: 01	**COPY NO:**

Statement of Applicability

Current as of: 30th October, 2021

Legend (for Selected Controls and Reasons for controls selection)

LR: **legal requirements,**CO: **contractual obligations,**BR/BP: **business requirements/adopted best practices,**RRA: **results of risk assessment,**TSE: to some extent

ISO/IEC 27001:2013 Annex A controls			Current controls	Remarks (with justification for exclusions)	Selected controls and reasons for				Remarks (overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	**Sec**	**Control Objective/Control**							
5 Security Policies	5.1	Management direction for information							
	5.1.1	Policies for information	X				X		ICT POLICY (KNP /MR/ICTP/05)
	5.1.2	Review of the policies for information security	N/A				X		ICT POLICY 20.0
6 Organisation of information security	6.1	Internal organisation							
	6.1.1	Information security roles and responsibilities	X				X		HR Manual 18.11
	6.1.2	Segregation of duties	X				X		IN PRACTICE
	6.1.3	Contact with authorities	X				X		IN PLACE
	6.1.4	Contact with special interest groups	X		X				IN PLACE
	6.1.5	Information security in project management	X		X				IN PLACE (Projects Implementation Committtee)
	6.2	Mobile devices and teleworking							
	6.2.1	Mobile device policy	X				X		HR MANUAL 20.4
	6.2.2	Teleworking	X				X		HR MANUAL 20.6
7 Human resource security	7.1	Prior to employment							
	7.1.1	Screening	X		X		X		HR MANUAL 2.8
	7.1.2	Terms and conditions of employment	X		X		X		HR MANUAL 2.0
	7.2	During employment							
	7.2.1	Management responsibilities	X				X		HR MANUAL 2.8
	7.2.2	Information security awareness, education and training	X		X				HR MANUAL 2.8
	7.2.3	Disciplinary process	X		X				HR MANUAL 13.13.2

	7.3	Termination and change of employment							
	7.3.1	Termination or change of employment responsibilities	X						HR MANUAL 18.2.2
8 Asset management	8.1	Responsibility for assets							
	8.1.1	Inventory of assets	X		X		X		ICT policy 5.6.2
	8.1.2	Ownership of assets	X				X		INTERNAL AUDITOR/PRINCIPAL
	8.1.3	Acceptable use of assets	X				X		ICT POLICY 5.2.1
	8.1.4	Return of assets	X				X		HR POLICY 18.7
	8.2	Information classification							
	8.2.1	Classification of information	X				X		procedure for documented information
	8.2.2	Labeling of information	X				X		procedure for documented information
	8.2.3	Handling of assets	X						HR POLICY 7.2; 15.5
	8.3	Media handling							
	8.3.1	Management of removable media	X				X		ICT POLICY 10.2
	8.3.2	Disposal of media	X				X		ICT POLICY 10.3
	8.3.3	Physical media transfer	X				X		ICT POLICY 10.4
9 Access control	9.1	Business requirements of access control							
	9.1.1	Access control policy	X		X				ICT POLICY 5.7
	9.1.2	Access to networks and network services	X		X				ICT POLICY 5.9
	9.2	User access management							
	9.2.1	User registration and de-registration	X		X				ICT POLICY 7.0
	9.2.2	User access provisioning	X		X				ICT POLICY 7.0
	9.2.3	Management of privileged access rights	X				X		ICT POLICY 7.0
	9.2.4	Management of secret authentication information of users	X				X		ICT POLICY 5.3
	9.2.5	Review of user access rights	X				X		ICT POLICY 7.0
	9.2.6	Removal or adjustment of access rights	X				X		ICT POLICY 7.0
	9.3	User responsibilities							

	9.3.1	Use of secret authentication information	X		X				ICT POLICY 5.3
	9.4	System and application access control							
	9.4.1	Information access restriction	X				X		ICT POLICY 5.7
	9.4.2	Secure log-on procedures	X				X		ICT POLICY 9.2
	9.4.3	Password management system	X				X		ICT POLICY 5.3
	9.4.4	Use of privileged utility programs	X				X		ICT POLICY 5.7.2
	9.4.5	Access control to program source code	N/A						
10 Cryptography	10.1	Cryptographic controls	N/A						
	10.1.1	Policy on the use of cryptographic controls							
	10.1.2	Key management							
11 Physical and environmental security	11.1	Secure areas							ICT POLICY 5.7
	11.1.1	Physical security perimeter	X				X		AVAILABLE
	11.1.2	Physical entry controls	X				X		ICT POLICY 5.8g; 5.9
	11.1.3	Securing office, room and facilities	X				X		ICT POLICY 5.7.1
	11.1.4	Protecting against external end environmental threats	X				X		ICT POLICY 5.7.1
	11.1.5	Working in secure areas	X				X		ICT POLICY 5.7
	11.1.6	Delivery and loading areas	N/A						
	11.2	Equipment							
	11.2.1	Equipment siting and protection	X				X		AVAILABLE
	11.2.2	Supporting utilities	X				X		AVAILABLE
	11.2.3	Cabling security	NOT				X		ICT POLICY 5.9
	11.2.4	Equipment maintenance	X				X		ICT POLICY 5.6.3
	11.2.5	Removal of assets	X				X		ICT POLICY 1.4(ii)
	11.2.6	Security of equipment and assets off-premises	X				X		ICT POLICY 10.4
	11.2.7	Secure disposal or re-use of equipment	X				X		ICT POLICY 10.3
	11.2.8	Unattended user equipment	X				X		ICT POLICY 5.6.2
	11.2.9	Clear desk and clear screen policy	X				X		HR MANUAL 20.2
	12.1	Operational procedures and							
	12.1.1	Documented operating procedures	X				X		Functional areas & Management Rep

12 Operations security	12.1.1	Change management	X				X		HR POLICY Clause18; ICT Policy 16.7
	12.1.3	Capacity management	X				X		ICT POLICY Clause 7
	12.1.4	Separation of development, testing and operational environments	N/A						
	12.2	Protection from malware							
	12.2.1	Controls against malware	X				X		ICT POLICY 15.0
	12.3	Backup							
	12.3.1	Information backup	X				X		ICT POLICY 8.0
	12.4	Logging and monitoring							
	12.4.1	Event logging	X				X		ICT POLICY 9.0
	12.4.2	Protection of log information	X				X		ICT POLICY 9.2
	12.4.3	Administrator and operator logs	X				X		ICT POLICY 9.2
	12.4.4	Clock synchronisaton	X						ICT POLICY 9.2
	12.5	Control of operational software							
	12.5.1	Installation of software on operational systems	X				X		ICT POLICY 16.0
	12.6	Technical vulnerability management							
	12.6.1	Management of technical vulnerabilities	X				X		ICT POLICY 16.3
	12.6.2	Restrictions on software installation	X				X		ICT POLICY 16.4
	12.7	Information systems audit considerations							
	12.7.1	Information systems audit controls	X				X		ICT POLICY 5.7.2
13 Communications security	13.1	Network security management							
	13.1.1	Network controls	X				X		ICT POLICY 5.9
	13.1.2	Security of network services	X				X		ICT POLICY 5.9
	13.1.3	Segregation in networks	X				X		ICT POLICY 5.9.1
	13.2	Information transfer							
	13.2.1	Information transfer policies and procedures	X				X		ACCESS TO INFORMATION POLICY KNP/AIP/11
	13.2.2	Agreements on information transfer	X				X		ACCESS TO INFORMATION POLICY Clause 4.0
	13.2.3	Electronic messaging	X				X		ICT POLICY 1.4 (vi)

	13.2.4	Confidentiality or non-disclosure agreements	X						"
14 System acquisition, development and maintenance	14.1	Security requirements of information							
	14.1.1	analysis and specification	X				X		ICT POLICY 6.3.1
	14.1.2	Securing applications services on public networks	X				X		ICT POLICY 5.9
	14.1.3	Protecting application services transactions	X				X		ICT POLICY 12.1.4
	14.2	Security in development and support processes							
	14.2.1	Secure development policy		EXCLUDED					WE DO NOT DEVELOP SOFTWARES
	14.2.2	System change control procedures		//					
	14.2.3	Technical review of applications after operating platform changes	X				X		ICT POLICY 16.8
	14.2.4	Restrictions on changes to software packages		//					WE DO NOT DEVLOP SOFTWARES
	14.2.5	Secure system engineering principles		//					//
	14.2.6	Secure development environment		//					//
	14.2.7	Outsourced development	X				X		ICT POLICY 12.0
	14.2.8	System security testing		//					
	14.2.9	System acceptance testing	X				X		ICT POLICY 16.0
	14.3	Test data							
	14.3.1	Protection of test data	X				X		ICT POLICY 13.4.1
15 Supplier relationships	15.1	Information security in supplier							
	15.1.1	Information security policy for supplier relationships	X				X		ICT POLICY 16.2.10(xii)
	15.1.2	Addressing security within supplier agreements	X						ICT POLICY 12.1.4
	15.1.3	Information and communication technology supply chain	X						
	15.2	Supplier service delivery management							
	15.2.1	Monitoring and review of supplier services							ICT POLICY 16.2.10(xii)
	15.2.2	Managing changes to supplier services							ICT POLICY 16.2.10(xii)

16 Information security incident management	16.1	Management of information security incidents and improvements							ICT POLICY 16.3.1
	16.1.1	Responsibilities and procedures	X				X		"
	16.1.2	Reporting information security events	X				X		"
	16.1.3	Reporting information security weaknesses	X				X		"
	16.1.4	Assessment of and decision on	X				X		"
	16.1.5	Response to information security incidents	X				X		"
	16.1.6	Learning from information security incidents	X				X		"
	16.1.7	Collection of evidence	X				X		"
17 Information security aspects of business continuity management	17.1	Information security continuity							KNP STRATEGIC PLAN
	17.1.1	Planning information security continuity	X				X		"
	17.1.2	Implementing information security continuity					X		"
	17.1.3	Verify, review and evaluate information security continuity					X		"
	17.2	Redundancies							
	17.2.1	Availability of information processing facilities	X				X		ICT POLICY
18 Compliance	18.1	Compliance with legal and contractual							
	18.1.1	Identification of applicable legislation and contractual requirements	X				X		
	18.1.2	Intellectual property rights	X				X		RESEARCH POLICY Clause 5.0
	18.1.3	Protection of records	X				X		HR MANUAL 15.3
	18.1.4	identifiable information	X				X		ACCESS TO INFORMATION
	18.1.5	Regulation of cryptographic controls	N/A						
	18.2	Information security reviews							
	18.2.1	Independent review of information security	X				X		MR SCHEDULES/ AUDIT

	18.2.1	Compliance with security policies and standards	X				X		MR SCHEDULES /AUDIT
	18.2.3	Technical compliance review	X				X		MANAGEMENT REVIEWS